مراكش - ورشة عمل DNSsec
الأربعاء، 09 مارس، 2016 – من الساعة 09:00 ص إلى الساعة 3:15 م بتوقيت غرب أوروبا
اجتماع ICANN رقم 55 | مراكش، المغرب

سيدة غير معروفة: ca. كندا.

شخص غير محدد: شكرًا. [غير مسموع] من، أعيش في الولايات المتحدة، وأشارك في DNSsec منذ الألفية السابقة.

سيدة غير معروفة: [غير مسموع]، الولايات المتحدة.

شخص غير محدد: مرحبًا، [غير مسموع] من ccTLD tr.

فيكي ريسك: فيكي ريسك من ISC ونحن ننفذ DNSSEC منذ 2006، ولا أصدق أنكم كنتم تقومون بها في الألفية السابقة.

راو نافيد بن رايس: نافيد بن رايس، باكستان، جامعة كابيتال.

نيل: [نيل جينس] من [غير مسموع]، الإمارات العربية المتحدة، ونحن نتولى حماية المفاتيح منذ الستينيات.

جون تشاند: جون تشاند من فيجي. زميل في ICANN.

وليام ستوك: وليام ستوك، من جنوب أفريقيا. ICANN في دراسة DNS بأفريقيا.

شخص غير محدد: حسنًا، جيد. لدينا عدد أكبر من الزملاء هنا.

[بن]: بن [غير مسموع]، مختبرات.

شخص غير محدد: [غير مسموع]، مختبرات. DNSsec قبل توحيدها.

شخص غير محدد: [غير مسموع] من [غير مسموع] زامبيا.

سيمون بال ثازار: سيمون بال ثازار، tz.، تنزانيا.

سونام كيبا: مرحبًا بكم جميعًا. أنا سونام من بوتان، وأتيت هنا من DNSsec لأننا لم ننفذ DNSsec في دولتي، لذا أود أن أتوصل لمعرفة شيء ما. شكرًا.

راجيوا أبيجوناراثنا: أنا رأجيوا من سريلانكا. زميل في ICANN. أجل.

شخص غير محدد: [غير مسموع] [زيتشاريا] من المغرب.

شخص غير محدد: [غير مسموع] [محمد] من المغرب.

شخص غير محدد: ممتاز. هل ثمة أحد آخر؟ هل تريد أن تصرخ باسمك فحسب؟ هنا.

شخص غير محدد: لم أجري هذا الصباح.

شخص غير محدد: [غير مسموع] ru.

شخص غير محدد: حسنًا. هل ثمة أحد آخر؟

شخص غير محدد: حسنًا، هيا لنبدأ.

خوزيه أورزوا: خوزيه أورزوا من cl.

شخص غير محدد: cz.؟ سي، حسنًا. ماذا؟

شخص غير محدد: [غير مسموع] من سجل in. [غير مسموع] الهند.

شخص غير محدد: نعم، رائع. هل نسينا أي شخص. حسنًا، داني.

داني جرانت: ما هو الطلب؟

شخص غير محدد: من أنت ومن أين؟

داني جرانت: من أنا؟ أنا داني. وأنا من CloudFlare.

شخص غير محدد: هل يود أي شخص آخر أن يتدخل؟ أوه، حسنًا. قل مرحبًا ومن أين أنت.

سارة مونتيرو: أنا سارة. وأنا من pt. البرتغال.

شخص غير محدد: ممتاز. هل نسينا أي شخص آخر؟

برام فودزولاني: أنا برام فودزولاني من مالاوي.

شخص غير محدد: رائع. وعلينا القيام بهذا أكثر من ذلك. كان الأمر رائعًا. ويجب علينا القيام بذلك. حسنًا، وروبرت هنا. مرحبًا يا روبرت.

روبرت مارتن ليجين: أقدم نفسي. أنا روبرت مارتن ليجين من باكيت كليرينج هاوس.

شخص غير محدد: حسنًا، لنبدأ. هل تود قول مرحبًا؟ أو التعريف بنفسك؟ لا. حسنًا.

شخص غير محدد: حسنًا. حسنًا، مرحبًا بالجميع، في ورشة عمل DNSsec. وقد كان هذا بالفعل وقتًا جيدًا نحتاج فيه للقيام بذلك. وكان هذا جيد حقًا. جولي، نود الاعتماد على ذلك في وقت ما للمرة القادمة أيضًا. لذا، أنا كنت سأستعير هذا من كاثي، فأنا على وشك كتابة شيء مفيد.

عليكم رؤية أحد ما يقوله أندرو. وبالنسبة للجد هنا على ورشة عمل DNSsec فقد التزمتم الآن بالبقاء في هذه القاعة حتى 2:15 من عصر اليوم. ست ساعات إضافية بالفعل، وأنتم لا. يمكنكم المغادرة. يوضح هذا ترتيب موعد ظهور عروضنا لما نقوم به. ونرحب ببقائكم بأقصى ما يمكن أو في الفعالية حسب اهتمامكم كما أن جولي تريد أن تقول شيئًا.

جولي هيدلوند: سأعلمكم فقط بالغداء، فسوف تستلمون بطاقة الغداء التي بها خريطة على الخلف. ولن يكون الغداء هنا، وهو ما يسعدكم معرفته. حيث سيكون بالخارج في مكان رائع ولكنه ليس قريبًا. لذا، نحن نمنحكم حوالي 10 دقائق أو ما شابه للذهاب إلى الغداء وستعرض الخريطة كيفية القيام بهذا. وسيكون هذا رائعًا حيث يوجد مرشدين ولافتات طوال الطريق. ولقد اشتريتم بالفعل التذكرة. لذا، احتفظوا بالتذكرة حتى إذا قررتم الذهاب إلى مكان ما آخر هذا الصياح. إن أردتم الغداء، فاحتفظوا بالتذكرة. شكرًا.

دان يورك: لذا، سأشير فقط إلى المتحدثين، روس موندي موجود لدينا هنا. ولديه جهاز الآيباد الصغير الذي يتضمن مؤقتًا. لذا، نحاول الحفاظ على الوقت مع تقدمنا في هذا مع مراعاة بالطبع أننا بدأنا الاجتماع متأخرًا 15 دقيقة. ولكن سأطلب من الناس الحديث فقط أسرع أو ما شابه.

لذا، سأتطرق إلى بضعة شرائح سريعة هنا. واسمي مرة أخرى هو دان يورك. وأنا جزء من لجنة البرنامج، الشرائح لا تعمل. حسنًا، إنها ليست هنا. فلماذا لا نضغط على الأزرار أو ما شابه. هل هذا متصل؟ حسنا، انظروا. زر التشغيل. مرحى. دعونا نقوم بذلك مرة أخرى.

حسنًا. كيف نترجم ووهو؟ لا، إنه يهز رأسه. حسنًا. الآن، نضعه في الوضع، حسنًا، هنا. أجل. وسنذهب إلى قائمة العرض [غير مسموع]. سأنطلق. حسنًا. لذا، دعونا نرى ما إذا كان سيعمل. ها نحن ذا. لا. حسنًا. ودعونا نستخدم الشرائح. لنبدأ. الشريحة التالية.

لذا، نظريًا، فإن الشرائح والملفات الصوتية في هذا الرابط. ونظريًا أيضًا، من المفترض أن نجد مقاطع الفيديو على يوتيوب. ولا نزال نؤكد ما إذا كانت هناك بالفعل. ولكن هل هي هناك؟ إنها تبث على Adobe Connect لذا فلن يكون بث اليوتيوب هناك. حسنًا. يقول السيد أنها تبث على Adobe. ولكنها لا تعمل. نعم، ولكن هل لدينا روابط يوتيوب؟ لا، أبدًا. حسنًا. وليس لدينا هذه الروابط. لا بأس. لا بد أنها متروكة من، حسنًا، لا بأس. حسنًا. لقد حدث لدينا عطل. كان هذا من 54 في دبلن حيث ألقينا هذه بسرعة. لذا، يمكنكم الحصول على هذا من خلال غرفة Adobe Connect، وتجاهل هذه الروابط على يوتيوب. لنتابع.

كذلك، هناك لجنة برنامج تشكل جزءًا من هذا. فما عدد أعضاء لجنة البرنامج الموجودين؟ فقط ارفع يدك أو ما شابه. حسنًا. عدد الزملاء المشاركين في هذا يرتبط بما يجري.

لذا، فنحن من يجمع هذا، والبرنامج هنا، وسننظر أيضًا، عقب هذا، في العروض للمرة القادمة مهما يكن الموقع المعلن رسميًا. لذا، في ICANN 56. حسنًا، يعرف الموقع رسميًا باسم بنما. الشريحة التالية.

نحن ممتنون للغاية للرعاة الذين تسببوا في هذا. وأعتقد Afilias، هل لدينا أي شخص من Afilias في القاعة؟ لا، سيكون جيم هنا، وربما سيكون هنا في وقت ما. سارة، لدينا جاك وماذا؟ أماندا، نعم، وهي موجودة. ليس Dyn، لا أعتقد أن أي شخص من Dyn ولكن SIDN، أعرف كريستان كان هنا. نعم هذا هو، هناك.

لذا، إن كانت لديكم فرص عليكم توجيه الشكر إلى هؤلاء الأشخاص لأنهم من ساعدوا في توفير الغداء. حسنًا. لذا، وإن كنتم [غير مسموع].

شخص غير محدد: [غير مسموع] الانتظار بعد الغداء [غير مسموع].

دان يورك: سأشكرهم الآن، إذًا. حسنًا، التالي. نريد أيضًا أن نشكر Afilias على التواجد المساعدة في تجميع جهات تنفيذ DNSsec. كان هنا عدد من الناس. فمن كان هنا. كان هنا عدد من الناس. حسنًا. للعلم في المستقبل، أيضًا، لدينا تجمع مساء الاثنين لكل اجتماع ICANN. الشريحة التالية من فضلك.

وهذه صورة لطيفة. حسنًا، ليست هذه مجموعة الشرائح. أوه. أجل. حسنًا. حسنًا.

شخص غير محدد: نعم. المرة التالية، أعتقد في الاجتماع ب، يوم فني وستعمل DNSsec عن قرب معًا، حتى يمكننا أن ننظر فيما إذا يمكننا دفع شيء من البدلات اليومية الموضوعة في [غير مسموع].

دان يورك: يبدو ذلك جيدًا. وأيضًا، أود أن أقول فقط، بالمناسبة، أن الدكتور إبرهارد ليسيه هنا، وهو ينظم اليوم الفني. وأشجعكم على العودة والنظر في الأرشيف بحثًا عن هذا، لأن السيد هنا من dot TR، أتيلا، قدم عرضًا ممتازًا حول الحرمان المنتشر للخدمة الذي حدث في تركيا. ولا يتعلق الأمر مباشرة بامتدادات DNSsec ولكنه عرض ممتازًا. إذن، تفضل.

شخص غير محدد: لقد كان رئيسي. أنا لست من يقدم العرض.

دان يورك: نعم، معذرة. أنا أحيركم.

شخص غير محدد: وهو [غير مسموع] عني.

دان يورك: حسنًا، معذرة. حسنًا. على أية حال. لقد كان عرضًا رائعًا من dot TR. ويمكنكم الاطلاع عليه. فهو جيد. أيضًا، قدم السيد بالخلف هنا من تنزانيا عرضًا جيدًا، يبدو مثل "ماذا؟" في المنتدى الأفريقي لنظام اسم النطاق، حيث قدم خطابا رائعًا حول ما يقوم به لتنفيذ DNSsec وكافة التقنيات الأخرى في موضعه، لذا، فهذا أمر جيد أيضًا. وعلينا أن نحصل على هذه الروابط. حسنًا. فلننتقل إلى الصورة التالية.

طرحت ورشة العمل هذه علينا من قبل اللجنة الاستشارية للأمن والاستقرار في ICANN مع مساعدة إضافية من برنامج النشر الشامل في مجتمع الإنترنت وهي كيفية مشاركة مع بعض هذا. لذلك هذا شيء جيد يجب أن نلاحظه. لنتابع.

هذه جدول الأعمال، ولديكم نسخة طبيعة أمامكم الآن، وستقدم لكم قراءة أفضل لهذا. يعتبر مغزى ذلفك أنلدينا فيكي أولاً وسيقدم لنا تحديثا حول DLV، كما لدينا بعدها مجموعة رائعة أتطلع إليها، ويتحدث العديد من الأشخاص هنا بالفعل عن DNSsec في أفريقيا.

لذا، سيكون لدينا عرض من ألين بشأن تحول DNSsec أو علامة التحول. كذلك، لدينا داني هنا للحديث عن جهود CloudFlare لتنفيذ DNSsec وفق المعايير. بعد ذلك، بالنسبة لمن لم يشاركوا، فلدينا استعلام DNSsec رائع، وسيكون تحدٍ لكم في هذا الوقت. وقد قام روي آريندس بذلك، وستحصلون على سمعة رائعة، أليس كذلك؟ لأنه من فاز في 54؟ هل نتذكر؟ لا أتذكر. هل هو من فاز؟ لا أعرف. [غير مسموع] ستكونون مشهورين في العالم.

وبعد الغداء، لدينا لجنة من الزملاء ستتحدث عن كيفية تحديد التشفير في DNSsec ولدينا بعض العروض الرائعة تتحدث عن ذلك. كما سندور طوال اليوم مع نقاش حول استبدال KSK وما يلزم حدوثه هناك.

الشريحة التالية، من فضلك. الشريحة التالية الآن. أوه، جولي تقول شيئًا ما. لا، أبدًا. حسنًا. حسنًا. لذا، نحن مستعدون للحظة أثناء حصولنا على الصور الصحيحة ولكننا لن نعرض عليكم الأمور الصحية على الشاشة ولذا، سيكون هذا سيئًا. لا تريدون القيام بهذا. لذا، انقر فوق فريق الرقص.

حسنًا. هل يرغب أي شخص في الحديث عن أي شيء آخر؟ روبرت، ما هو الرائع هنا، حسنًا، أعرف. أعتقد أننا في افريقيا، لذا، لا بد أن القاعة ساخنة. وعادة، تكون باردة، اليس كذلك؟ حسنًا. أعتذر لروابط يوتيوب، يا جولي. وأعرف من أين أتت. كان هذه آخر مرة في دبلن، لأننا لم يكن لدينا كاميرا، لذا، ألقيت كاميرا سريعة. ولم تكن بهذه الكفاءة.

وجولي تتسم بفعالية رائعة لكافة هذا، ولذا، فقد حدثت ذلك بروابط مماثلة، ولكني لم أدرك أن هذه الروابط معي، وهذا ليس أنا بالفعل. لذا، سأترك الإعلان عن الروابط الخاطئة. عذرًا على هذا، هل يسمع أي شخص عن بعد. حسنًا.

نعم، إنه يعمل. ما حدث المرة السابقة كان أننا تجمعنا في غرفة غريبة في الطابق الرابع من مركز دبلن للمؤتمرات الذي كان مفتوحًا للغاية، ولا توجد كاميرات. وبهذا، شاركنا ولم تكن هناك طريقة لعرض الفيديو. كما أننا قمنا بما استخدمت الكاميرا بالفعل له بسرعة وذهبنا إلى حساب يوتيوب لمجتمع الإنترنت، ونحن نبث هذا.

واليوم، لدينا بالفعل كاميرا، بالرغم من أنها في لابتوب هنا يبث الفيديو، لذا يمكن بالفعل رؤيتنا في هذا الوقت. حسنًا. ها نحن ذا. وحسنًا، لنعرض الصورة. علينا عرض الصورة. لذا، دعونا نعرض الصورة هنا. ها نحن ذا.

هلا نرجع إلى الشريحة السابقة. لقد عرفت هذا. فها نحن نبدأ. لذا، نحن، ولأن كريستيان أظهر هذا الشعار هنا، حسنًا؟ وهذا جانب مهم للغاية. حسنًا؟ يعتبر SIDN شعارًا جديدًا، أليس كذلك؟ لذا، نحن أيضًا، ونبحث عن ممول خامس، شركة ترغب في المساعدة في

تمويل هذه الفعاليات مع تقدمنا هنا. لديكم فرصة الإدراج هنا وعلى بطاقات الغداء والأشياء الأخرى. ويمكنكم أيضًا المساعدة، مع الامتنان الكبير لهذا المجتمع للمساعدة في تمويل الغداء.

وذلك بمبلغ 2000 دولار لبقية السنة وبالدولار الأمريكية. كذلك، أود الحدث إلى أي شخص مهتم بالقيام بهذا. ونحن نقدر للغاية الممولين، ونود وجود ممول خامس لأنه في بعض الأحيان عند الذهاب إلى الأماكن، فهذا يكلف قدرًا كبيرًا من المال حتى نتمكن من الوصول إلى القاعة والغداء وكل شيء آخر نود القيام به.

لذا، دعونا ننتقل إلى الشريحة التالية حيث لدينا الصورة. وكان هناك بعض الأشخاص. حسنًا. وكان لدينا حوارًا رائعًا، ووقتًا رائعًا للحدث عن الأشخاص. كما تم تطوير المشروعات من هذه التجمعات. ولدينا بالفعل كثير من المتعة في الحديث معًا. لنتابع. التالي.

حسنًا، التالي. نعم التالية. حسنًا، هيا لنبدأ. التالي. لذا، نريد الحديث عن الإحصائيات حول DNSsec والخرائط وبعض الأجزاء الموجودة هنا بهذا الشأن. كما نذكر الأشخاص أنه عند الحديث، فهناك شريحتان بشأن DNSsec، أليس كذلك؟ وهذا جانب التوقيع وهناك جانب خاص بالتقييم. كما أن أحدها هو إنشاء التوقيعات، والتحقق منها. لذا، دعونا نتعرض لهذا.

ولذا، دعونا ننظر في هذا ولدينا أولاً من جيف هيوستون، الجالس في الزاوية هناك. ولدينا هذه الخرائط الرائعة وهذه الشرائح متوفرة على موقع ICANN، ولذا، يمكنكم الاطلاع عليها ويمكنكم أيضًا الاطلاع على عناوين URL التي قدمتها لموضعهم. ولكن خريطة جيوف توضح الزيادة المتواصلة في التحقق من DNSsec عالميًا. لذا، نرى زيادة في مقدار التحقق هنا.

والانخفاض الكبير في الوسط في سبتمبر، لذا، أعادت جوجل تكرار هذا بالطريقة التي يقومون بها بالإعلانات وما شابه وهو ما يستخدمه جيوف لعد هذا. ولذا، هناك انخفاض في هذا ولكنه جيد. نعود إلى التوجه. حسناً؟ الشريحة التالية من فضلك.

كانت هذه قائمة، وهو ما يصعب قراءته من هذا العرض. أعتقد أني أحتاج لوصفة عيون جديدة. ولكن أحد الأمور المثيرة هي أن هناك عرض كلي للعالم الذي يجري فيه التحقق. والأمر الشيق هو أنه إذا نظرتم في أعلى ذلك، فإن بعض المناطق من العالم التي كان لديها أعلى مستوى من تحقق DNSsec توجد في أفريقيا، للأسباب التي سنتعرض لها في موضع آخر.

ولكن، يمكنكم أن تروا نوع المواطن التي نراها مستوى أعلى، حوالي 30، ما هذا؟ 34% في الأعلى هناك. حسنًا. فلننتقل إلى الشريحة التالية. كان هناك المنظور العالمي الشامل حول التحقق من DNSsec، وملاحظة أن أفريقيا مرتفع إلى حد ما.

الآن، إذا بدأت الدخول في ذلك بقدر من التفصيل، فيمكنكم رؤية أنه استخدام مرتفع أيضًا لخادم DNS العام من جوجل، وهو 8.8.8 والمرتبط بكل من IPv4 وIPv6، وهذا قليل مما يجري. وإذا نظرنا في الصورة القادمة، حسنًا، لا يمكن قراءتها من هنا. حسنًا. لا بأس.

ولكن إذا انتقلنا إلى URL ونظرنا في شرائح جيوف، أو الإحصائيات فسترون أن ما يحدث هو أن بعض الدول الموجودة هنا لديها نسبة مرتفعة من التحقق، ولكن جزء من هذا يرجع إلى أن لديهم استخدام مرتفع لنظام DNS العام في جوجل.

فالدولة الرابعة هنا مع ذلك هي مدغشقر، مع ملاحظها أن لديها استخدام فقط بنسبة 8% لنظام DNS العام، وكذلك الخاص بجوجل مما يعني أن 92% الأخرى في التحقق من DNSsec تحدث ضمن مزودي ISP هناك في مدغشقر، لذا، فهذا ضخم وهو رائع. فنحن نحب رؤية هذا النوع من الأمور تحدث.

لذا، ما يجري هو أخبار جيدة. ودعونا نتحدث في الجانب الموضح. هذا هو تقرير نشر ريك لامب يوضح نسبة نطاقات TLD الموقعة ككل. ونحن الآن في طريقنا إلى 80%. وبالطبع معظم ذلك هو نطاقات gTLD الجديدة الواردة، والموقعة افتراضيًا إلا أنه من الجيد رؤيتها. لنتابع. التالي.

حسنًا. لا يمكنني قراءة هذا من هنا، لذا ملاحظة للمرة القادمة، سأجعله أكبر قليلاً حتى أستطيع القراءة من على بعد خمسين قدمًا. ويمكنني الاقتراب. لدي الميكروفون في يدي، كما يخبرني روبرت. لذا، نعم يمكننا قراءة هذا، شكرًا لك روبرت على توضيح هذا. وربما تصل الحرارة إلي.

لذا، يمكنكم أن تروا هنا في الأعلى، NL تأتي في المقدمة بحوالي 44% من نطاقها موقعة، وأكثر من 2 مليون، لذا، المجد للزملاء من NL. هل هم هنا؟ أجل. يجب أن يكونوا هنا. أنتم هنا أيها السادة. عمل رائع. حسنًا؟

كما أن ممثل البرازيل هنا مع عدد كبير. وما قمت به في شريحة ريك هو أنكم نقرتم على، ليس بديهية. كذلك، سيخبركم ريك أنه ليس مصمم لديه خبرة مستخدم، ولكن إذا نقرتم فوق الإجمالي الموقع، إذا نقرتم فوقه مرتين، فسترتب بهذه الطريقة، ويمكنكم أن تروا ماذا يجري هناك.

كما نرى أيضًا هنا أن se.com تتضمن عدد كبير، بالرغم من أن النسبة صغيرة. ولذا، نبدأ في رؤية بعض الأمور الجيدة التي نبدأها لمعرفة بعض المقاييس حول نسبة المواقع الموجودة. الشريحة التالية من فضلك.

نريد الانتقال إلى الخرائط وبالنسبة لمن لا يعلمون، فقد صنفناها على خمسة مراحل من التجربة، التي نعرف بالأساس أنها تجري مع DNSsec بصورة ما. وأعلن أنهم قالوا أنهم سيقومون بهذا. جزئيًا، وقعت المنطقة ولكن ليس هناك DS في الجذر وبعدها يكون DS في الجذر ثم على المستوى التشغيلي. الشريحة التالية من فضلك.

أول التفاصيل التي أود طرحها هي بعض ما قلتم لي "حسنًا، لماذا لا تزال خارطة الطريق تعرض DS في الجذر، ولكن ليس المستوى التشغيلي؟" والإجابة هي لأني ليس لدي بالفعل طريقة سهلة للمعرفة إذا لم تخبروني أنكم تقبلون هذا. لذا، إذا كنتم ترون أنفسكم في DS أخضر فاتح في الجذر لكنكم تقبلون سجلات DS، دعوني أعرف. الشريحة التالية من فضلك.

لذا، هذه هي النظرة العامة على الخريطة. ونحن نحصر على مزيد من اللون الأخضر باستثناء ما يجري هنا. سنرى على أي حال. نعم، قليل من التفاصيل. وسوف نصل إلى هناك. الشريحة التالية من فضلك.

هذا ما تبدو عليه أفريقيا. الآن، هناك إضافة أخرى يجب أن نضعها هنا للزملاء في المغرب، تهانينا. فقد وقعتم على نطاق ma. لكنه كان موقعًا بعد أن نفذت هذه الخرائط. ولكنها ستكون الجولة التالية من الأمور الجارية. كما وقعت بتسوانا أيضًا هنا، لذا، فنحن نرى بعض التقدم في هذا، لكن بوضوح، هذه منطقة جيدة حيث يمكننا رؤية مزيد من النمو وأعرف أن ألين سيتحدث عن هذا، أو حسنًا، يشارك ألين هنا في البرنامج، وهو في DNSsec-Africa.org، التي تقوم بالكثير للمساعدة في توسعة النطاق هنا. لنتابع. التالي.

آسيا والمحيط الهادي، في المنطقة بصورة عامة، الشرق الأوسط، التغيير الوحيد منذ آخر مرة هو أن أذربيجان وقعت على az. أو AZ. التالي. ولم تتغير أوروبا منذ آخر مرة. التالي. ولا LAC. على أنها ستستمر جميعًا هناك. الشريحة التالية، من فضلك. وأمريكا الشمالية، هذا أنتم. الشريحة التالية، من فضلك.

لذا، تخرج هذه الخرائط كل يوم اثنين صباحًا. ونحن نحدثها وهي هناك. ويمكنكم الاشتراك. الشريحة التالية، من فضلك. لدينا تقويم فعاليات نحاول تحديثه مع فعاليات DNSsec. ونرحب بإرسال الاقتراحات، إن كان لديكم هذا. الشريحة التالية، من فضلك.

سأذكر أن هناك فعالية كبيرة مخصصة. ولدينا هذه بأن فريق عمل هندسة الإنترنت كان يقوم في نهاية الأسبوع قبل فريق عمل هندسة الإنترنت. وقد حدث، بدأ ذلك منذ بضعة مرات، وهناك مجموعة من الأشخاص مجتمعين في نهاية الأسبوع ويعملون على DNSsec DANE وكذلك سرية DNS وقد فازت مجموعتنا بالفعل بأعلى جوائز لآخر فعاليتين. فلدينا مجموعة هناك.

ولذا، هذه مجموعة أخرى ستجتمع. وإذا كنتم ستذهبون إلى فريق عمل هندسة الإنترنت، فأنتم تعرفون المطورين الذاهبين، ويريدون التشفير والعمل على مشاريع الأمن بخصوص DNS. ونرحب بوجودكم. يمكنكم متابعة الروابط. الشريحة التالية من فضلك.

والأمر الأخير هو أن هناك مشروع سجل DNSsec الذي يستمر في النظر في التعقيبات والمساهمات وهذا كل ما سأقوله. كما أننا سنتابع مع جولي التي تقول شيئًا ما.

جولي هيدلوند: لدينا سؤالان في غرفة الدردشة. الأول من ماركوس من Global Village. للديه سؤال أعتقد أنه يتعلق ببعض الإحصائيات التي عرضتم. وسؤاله هو "كيف يمكن أن يكون لدى مايوت معدل تحقق من DNSsec بنسبة 95% واستخدمت جوجل معدل 96%؟"

دان يورك: جيوف، هل تريد مني الإجابة على ذلك؟

جيوف هوستن: بالتأكيد. إنها أعلى قليلاً من جوجل بالفعل، لأن واحد أو اثنين من مزودي خدمات الإنترنت المحليين قد يجرون التحقق أيضًا.

دان يورك: وأعتقد أن هذه كانت الطريقة الأخرى.

جيوف هوستن: أوه، إنه أقل. حسنًا. لا، في بعض الأحيان يضع الزملاء أكثر من حل واحد في التكوين المحلي، و[غير مسموع] com . وهذه عادة الحالة التي قد يسرد فيها ISP بصورة مناسبة جوجل وربما طريقة حل أخرى. الآن، تتعلق المشكلة بخصوص DNSsec في أنه عند الانتقال إلى النطاق الموقع بصورة غير مناسبة، واختباري به واحد، فلن يقول "هذا موقع بصورة غير مناسبة."

والإجابة التي يتلقاها DNS هي "فشل الخادم." ولذا، إذا كان لديكم أكثر من جهة حل واحدة، فعند فشل الخادم، كما تعتقدون "حسنًا، يجب محاولة الجهة الأخرى." وإذا لم تتحقق الجهة من الإجابة، فسيتم تضليلكم وستنتقلون إلى نطاق موقع بصورة غير مناسبة بالفعل.

لذا، في هذه الحالة، يجب أن يكون هناك عدد من الزملاء يستخدمون جهة محلية بالإضافة إلى جوجل. وعند قول جوجل "لا يمكنني الذهاب هناك لأنه فشل خادم موقع بصورة غير مناسبة،" فهناك عدد آخر من الزلماء، "لدي إجابة أفضل، سآخذ الإجابة الممتدة." ومن الحماقة بالفعل القيام بهذا، لكن الناس تقوم بهذا.

دان يورك: حسنًا. شكرًا لك جيوف.

جيوف هوستن: جيوف.

دان يورك: السؤال الثاني، جولي.

جولي هيدلوند: وبالفعل، وجد هذا الشخص الإجابة التي كان يتطلع إليها، لذا، لقد انتهينا.

دان يورك: رائع. نحب هذا النوع من الأسئلة. حسنًا، مرحبًا بالجميع، في ورشة عمل DNSsec. الرجاء الشعور بالحرية، وقد رأيتم بالفعل الوافدون الجدد، وأنتم ترحبون بالفعل بالأسئلة في أي نقطة من الوقت. ولدينا عدد كبير من الأسئلة. لا تهمسوا كثيرًا. وسيسعدنا الحديث إليكم جميعًا بأي صورة أو شكل أو صيغة. لذا، رجاء توجيه الأسئلة.

وبهذا، فيكي، يمكنك إما الجلوس هنا أو استخدام الميكروفون، مهما يكنه ما تريدون القيام به، حسنًا. وليس لدينا نقر، لذا، كاثي. أجل. أيًا كان. وسنكتشف عمل جهاز النقر في نقطة ما هنا.

فيكي ريسك: مرحبًا. أنا فيكي ريسك من ISC. بالنسبة لمن لا يعرفون، فنحن ناشرو المصدر المفتوح من نظام BIND DNS. ولكن اليوم، سأتحدث عن DLV. تفضل.

لذا، DLV، ترمز إلى جهة التحقق من بيانات DNSsec. إنه شيء أنشأته ISC ويعود إلى 2006. وكانت الفكرة أن الأشخاص الذين أرادوا استخدام DNSsec قبل توقيع الجذر ونطاقات المستوى الأعلى يمكنهم استخدام DLV كنوع من الجهة الأصلية الراعية.

في هذه النقطة، كما سمعتم من دان، فإن نسبة كبيرة من نطاقات المستوى الأعلى موقعة وكذلك الجذر بالطبع. وبهذا، هناك إحساس أن DLV أنجزت بالفعل ما يمكنها المساعدة به في الاعتماد المبكر.

وأعتقد أنه سيكون هناك أشخاص يرون أن متابعة وجود هذا المسار البديل للتحقق من احتمالية DNSsec غير مشجع لبقية جهات الاعتماد. لذا، منذ سنة، بالفعل، في أول اجتماع ICANN في 2015، أعلنت ISC عن أننا نخطط لإيقاف DLV بنهاية سنة 2017. تفضل.

أعتذر عن الخط الصغير مرة أخرى. لذا، أعلنا عن هذا في ICANN في سنغافورة في فبراير الماضي. كذلك، لقد حدثنا الصفحة الرئيسية في موقع DLV، وقد وضعناها على الموقع الإلكتروني الخاص بنا، وأرسلناها إلى بعض القوائم البريدية للإنترنت، كما اتصلنا بجهات BIND، جهات تجهيز نظام التشغيل في برنامج BIND. كذلك، أعلنا في NANOG عن ذلك في بضعة مؤتمرات، وأرسلنا رسالة بريد إلكتروني إلى كل مستخدم في DLV.

بوضوح، نريد التأكد من أن الجميع يعلم أننا نخطط لإيقاف العمل قبل أن نوقف تشغيله. لذا، فخطتنا كانت أولاً، أن نبدأ بما نتوقع أنه سيكون عملية ممتدة لإثناء الناس عن الاستعلام عن DLV، لذا، فنحن نثنيهم عن وضع جهات الحل للاستعلام عن DLV. وبعد ذلك، نبدأ تدريجيًا في استبعاد المناطق وDLV مع الوقت.

كما تتمثل الخطة في أن نستمر في الإجابة على الاستعلامات في DLV بصورة غير محددة لأنه سيكون من الأفضل لجهة الحل أن تحصل على إجابة سلبية سريعة من عدم الحصول على إجابة وربما إعادة المحاولة عدة مرات. عفوًا، تفضل.

لذا، هذا مجرد مثال واحد على البريد الإلكتروني المرسل. وقد أرسلنا هذا في شهر يونيو السابق. كما أننا انتقلنا إلى نظامنا وتحققنا من رؤية كل مستخدم للمناطق الموجودة، سواء كانوا يعملون أم لا، وسواء كان يمكنهم التحقق من ذلك أم لا بدون DLV، وأرسلنا لهم المعلومات حول المناطق وطلبنا منهم استبعادها إن أمكن. تفضل.

لذا، لن أعرض لكم بضعة إجابات حصلنا عليها، وهي ممثلة كما أعتقد. هذه الواحدة، أعرف بالفعل من أين أتت. وهذا الشخص بالتحديد ملتزم بالغاية بامتدادات DNSsec، لكنه ليس لديه أي طريقة أخرى للوصول إلى المنطقة العكسية الموقعة. كما أن هناك العديد من الناس، اعتمادًا على موقعهم، ليس لديهم بالفعل خيار ISP، وهذا المستخدم ليس لديه طريقة أخرى لتوقيع المنطقة المقابلة. لننتقل إلى النقطة التالية.

هذا شخص آخر لديه مسار للتوقيع، ولكنهم لا يمكنهم الوصول إلى المنطقة الأم لقبول سجلات DS. وهناك اثنان من الردود الشائعة للغاية.

كذلك، فالسبب أني أطرح هذا العرض هو أني أدرك أن العديد منكم هنا في القاعة لهم تأثير على تحسين الموقف لهؤلاء المستخدمين الملتزمين في DNSsec، وبعضهم وقع على المناطق منذ 2006، ويواجه مقترح بعدم الأمن أثناء إيقاف تشغيل DLV. تفضل.

حتى الآن، حيث أننا بدأنا في أن نطلب من الناس استبعاد تفويضاتهم إن أمكنهم، فقد استبعدنا حوالي 800 منطقة عمل. وهناك الكثير من المناطق الأخرى التي لا تعمل. وأعتقد أن الكثير من الناس كانوا يستخدمون DLV كأداة تدريب. وتتمثل المشكلة في أن بقية المناطق التي تتجاوز 2000 قد لا يكون لديها خيار آخر للحفاظ على أمن DNSsec.

علاوة على هذا، قمنا بالفعل بنوع من توسعة الإطار الزمني عند التخطيط لتنظيف المناطق التي قد تتحقق بدون DLV. وفي الوقت الراهن، عندما ترون الخط الأزرق، فهذا هو موضعنا الآن. ونستعد لإيقاف تسجيل أي من المناطق الجديدة التي قد تتحقق بدون DLV. وكما ترون، النقطة النهائية هنا، يوليو 2017، وهذا هو الموعد الذي نخطط فيه لاستبعاد سجلات DLV المتبقية. كما أن هذا سيكون إخطارًا لمدة سنتين للأشخاص الذين تم استبعاد سجلاتهم، ولكن في هذه النقطة، مما يمكنني رؤيته، أعتقد أننا سنجبر الأشخاص بالأساس على عدم التأمين بالنسبة لمن ليس لديهم مسار آخر.

لذا، حتى الإخطار بسنتين ليس كافيًا بالضرورة، كما هو واضح. ولذا، تحدثنا عن السجلات في DLV. لذا، دعونا نتحدث الآن عن استفسارات جهة الحل إلى DLV. وهذه هي الجهات التي تحاول التحقق من DNSsec. حيث يضع الاستعلام من DLV عبئًا إضافيًا على هذه الجهات، وخاصة حيث أنه لا يوجد بالفعل عدد كبير من المناطق الموجودة، وهذا مستحسن للحد من تقدم هذه الاستعلامات.

وبالطبع بعد 2017، لم تكن لديهم أي مناطق على الإطلاق في DLV، لذا، فهذا دون فائدة تمامًا، لجهات الحل للاستعلام عن الأمر، لذا، نود إثنائهم عن هذا. باول [غير مسموع]، ليس هنا. حسنًا، عظيم. حسنًا على أي حال، أحد الزملاء الذين ساعدونا في هذا، الزملاء في Red Hat، استبعدوا الاستعلامات إلى DLV من التكوين الافتراضي وتكوين جهة الحل في التوزيع. وقد أنجزت عدد من جهات التجميع هذا. كذلك، فقد استبعد فريق التطوير غير الملزم هذا من التكوين الافتراضي، وأعتقد أنه وضح ملاحظة في الوثائق توصي بألا تستعلموا عن DLV. تفضل.

لذلك، الآن، نرى نصف عدد الاستعلامات التي كانت لدينا منذ سنة. ومرة أخرى، لقد ذكرت أن عملية إيقاف العمل ستكتمل في 2017، إلا أننا نتوقع أن يستمر وجود بعض الاستعلامات إلى DLV بعد ذلك، بحيث نترك الخدمة تعمل.

لذا، باختصار، أنشأت ISC DLV لتشجيع استخدام DNSsec. وفي هذه النقطة، نعتقد أنها قد أدت الغرض منها بالفعل. على أنها لم تكن حلاً لمشكلة نظامية بعدم دعم DNSsec عبر القطاع، ولذا مرة أخرى، نحن نخطط لإيقافها. أعتقد أنني انتهيت.

حسنًا، لقدر أردت أن أشكر Afilias على مدة المشروع. وقد وفرت Afilias الخدمات الثانوية لـ DLV على أنها تحصل على استعلامات أكثر من ISC. وهذا ما أردت توضيحه.

دان يورك: فيكي، سؤال واحد فقط. لذا، اعتبارًا من يوليو 2017، هل ستبقى DLV تعمل أم لا؟

فيكي ريسك: ستجيب على الاستعلامات لكن بدون أي مناطق فيها.

دان يورك: لن يكون هناك مزيد من المناطق في DLV، حسنًا.

فيكي ريسك: صحيح. سنستمر في الإجابة على الاستعلامات فقط لأنها ستتيح لجهات الحل الحركة أسرع قليلاً.

دان يورك: حسنًا. ولكن، سيتم تفعيل إغلاق خدمة DLV اعتبارًا من يوليو 2017.

فيكي ريسك: نعم.

دان يورك: شكرًا. هل ثمة أسئلة موجّهة للزملاء؟ حسنًا. روس ثم ألين.

روس موندي: شكراً فيكي على هذا العرض. أقدر ذلك حقًا. أحد الأمور التي أود التأكيد عليها هنا للجميع في القاعة وإذا كنتم بالفعل في جلسة المبتدئين، فقد سمعتموني أتحدث عن ذلك، وهي أن الناس في هذه القاعة، بغض النظر عما يقومون به في DNSsec، يستمرون في طلب المزيد والمزيد من دعم DNSsec، سواء من أمناء السجل أو السجلات أو البائعين.

يرجع هذا كما تقول فيكي، إلى أن هناك عدد من الأنشطة التي لن يمكنها القيام بالتحقق. وأفضل طريقة لاستخدام DNSsec بصورة أوسع عبر قطاع العمل هو وجود كافة المؤيدين لمختلف الوظائف المشاركة في DNS للقيام بالأمور المناسبة للتأكد من توفر DNS أو DNSsec لأي شخص يريد استخدامها. لذلك، اطرحوا الأسئلة. شكرًا.

فيكي ريسك: لذا، بالفعل، فقط للتأكيد على ذلك، أود أن أتمكن من إحالة هؤلاء الأشخاص إلى المشغل، ISP الذي يمكنه مساعدتهم في الحفاظ على سلسلة أمناء DNSsec بعد رفض DLV، وبعضها قد توصل إلى السؤال عن هذه المراجع. وهذا يحدث لي الآن، بالطبع، الإدراك المتأخر كبير بحيث إذا كنا نفرض رسوم على الناس لهذه الخدمة دائمًا، فيمكنهم أخذ هذه النقود في مكان آخر وإنشاء سوق لهذا، ولكنه ربما يكون متأخرًا.

دان يورك: آلين؟ أوه. لقد رأيت ألين أولاً.

آلين إينا: حسنًا، بالتأكيد. أشكر ISC على توفير هذه الخدمات لأنه أثناء النقاش الأولي، أعتقد أنه لم يكن من السهل حتى التوصل إلى إجماع في المجتمع الفني بشأن DLV. وأتمنى أن يكون لدينا أشخاص في هذه القاعة يمكنهم تذكر النقاش حول القائمة البريدية لامتداد DNS DNSOP. لذا، لكني أعتقد أنه كان مفيدًا للغاية، وشكرًا لكم، ISC، وربما نقول "مرحبًا،" لبول فيكسي [غير مسموع].

فيكي ريسك: شكرًا لك على ذلك. لم أكن في ISC في هذا الوقت، ولكني أخبرت أنه كان مثيرًا للجدال.

دان يورك: روبرت.

روبرت مارتن ليجين: أجل. أعتقد أنه من الجيد التعامل مع DLV. وبالنسبة للمستخدمين السعداء مع DLV، فإن التقنية لا تزال داخل البرامج المختلفة، على حد علمي. لذا، يمكن أن ينفذ الأشخاص DLV الخاص بهم، إن أرادوا هذا، بقدر ما أفهم.

ولكن هل لديكم أي فكرة عما تبقى هناك بالفعل؟ وهذا هو سبب أنها لا تزال هنا؟ يوجد الكثير من سجلات com. التي تدعم DNSsec على الإطلاق أم ماذا؟

فيكي ريسك: هناك عدد معقولة من المناطق المقابلة. وقد تحدثت إلى الزملاء من DE. كان هناك الكثير من الزملاء في التعليم وهي موجود بالفعل عبر الخريطة، بصراحة. كما أني لست متأكدًا من أني يمكنني أن أحدد بالضبط ما يجري. كذلك، هناك أشخاص يستخدمون ذلك كآلية انتقال عند الانتقال من مزود إلى آخر، وليس لديهم تعاون.

ولكن في الغالب كما أعتقد، أن التفويضات ليست مؤقتة بالفعل، لكنها لن تكون أمرًا واحدًا. هذا غير واضح. أعني، هناك بضعة أشخاص يديرون عدد من التفويضات هنا، ولكن في الغالب هي من واحد أو اثنين. [غير مسموع].

دان يورك: هل يود أي شخص آخر أن يتدخل؟

فيكي ريسك: أجل. أندري.

أندري: فقط لإنهاء الأمور. حسنًا، سؤالي هو أنكم خائفون من حدوث هذا عند إيقاف التشغيل. ولأن عدد الاستعلامات بالنسبة إلى K منخفضة العدد بالفعل، لذا لن يستخدم العديد من المستخدمين ذلك. وهناك العديد من المناطق المتاحة. وما سيحدث إذا تحولتم غدًا؟ أعتقد لا شيء. لذا، أعتقد أن لديكم الحرية في إيقاف DLV وفقًا لخطتكم.

ولكن السؤال الفعلي هو، لماذا لا نزال نتحدث عن ذلك؟ وهل أنتم خائفون مما سيحدث عند إيقاف DLV؟ لا أعتقد أنه سيكون هناك أي منها، حسنًا، مما يضر بسمعتكم، وهو الأمر الوحيد الذي قد يحدث. ولا أعتقد أنه سيحدث، لذا أعتقد أن لديكم الحرية في إيقافه.

فيكي ريسك: حسنًا، علي أن أخبركم أننا لم نحصل على أي خطابات حب حول ذلك. والأشخاص الموجودين في DLV غير سعداء بالفعل بهذا.

دان يورك: أية أسئلة أخرى؟

أندري: أعتقد أن الأشخاص سعداء بإنهاء هذا، لقد غادروا بالفعل.

فيكي ريسك: أجل، نعم.

دان يورك: وإذا كان هناك أي شخص وراء هذا، مهما يكن من يقوم بالأمر، ويريد الحديث، فالرجاء الظهور والصياح، ارفع يدك، قم بأي شيء. لدينا ميكروفون متنقل.

حسنًا. أريد الآن القول "شكرًا." وأود أن أردد كلمات ألين وأقول "شكرًا،" إلى فيكي في ISC على القيام بهذا. وقد كانت أداة للغاية أثناء الانتقال، لذا، شكرًا.

حسنًا. التالي، نحتاج لمجلس إقليمي هنا رجاءً. لذا، تقدموا للأمام وشاركونا، وسأحول هذا إلى مارك، الذي سيكون المشرف.

مارك إلكينز: طاب صباحكم جميعًا. اسمي مارك إلكينز. وأنا مشرف الجلسة القادمة. والعضو الأول لدينا يتقدم ببطء نحو المقدمة. وإذا كنا سنقوم بهذا من المقدمة، فيمكن للجميع أن يروا وجهك الجميل على الكاميرا. لذا، أول مقدم لدينا، ولدينا أربعة متحدثين بما في ذلك نفسي.

أول متحدث لدينا ألين إينا، نشط للغاية في المجتمع التقني في أفريقيا، ولديه شركاته المملوكة له. لذا، فهو بالتأكيد مشارك للغاية في AFNOG، وهي مؤسسة تدريب، مجموعة مشغلي الشبكات في افريقيا. لذا، كان أيضًا، لعدة سنوات منذ نوفمبر، مديرًا للمشاريع الخاصة في AFRINIC. وقد قضى الكثير من الوقت في موريشيوس للقيام بمختلف أمور DNSsec. لذلك، على سبيل المثال، لدى AFRINIC امتداد DNSsec للرد، بما في ذلك الإصدار السادس والقديم، وأنا سعيد للغاية بهذا. كما أنه بالتأكيد يعمل كمستشار ICANN بشأن مشروع عروض DNSsec وهو ما أعتقد أننا سنتحدث عنه.

آلين إينا: نعم. شكرًا لك، مارك. لذا سأتحول إلى اللغة الفرنسية. حسنًا، لا، دعوني [غير مسموع]، ولكن ليس لدى العديد من الأشخاص هنا، حسنًا.

مارك إلكينز: يمكننا وضع السماعات إن أردت. إن كنتم تشعرون بمزيد من الراحة، يمكننا --

آلين إينا: حسنًا. سأتحدث الإنجليزية. أجل. شكرًا لك، مارك. كما قلت، أنا أتحدث هنا كمستشار ICANN بشأن عروض DNSsec في أفريقيا. ومما يعرض بعد ذلك في الخريطة، يمكنكم أن تروا أن أفريقيا متأخرة من حيث نطاقات ccTLD واعتماد DNSsec.

وعلي أن أقول أنه ما رأيتم في 2015 أفضل مما كان الأمر في 2013 عندما بدأنا هذه الامور، لكننا لا يزال لدينا طريق طويل لنقطعه. لذا، العروض، عروض DNSsec هي واحدة داخل المدينة في جزء من إستراتيجية ICANN الأفريقية. وبعد ذلك، نحاول أن نساعد نطاقات ccTLD في أفريقيا لفهم ما هي DNSsec وكيف يمكن أن تحسن الخدمات المقدمة للمجتمع وما إلى ذلك.

لكن، لم يكن هذا سهلاً. وليس ذلك من السهل على الأطلاق لأننا نعرف جميعًا أن DNSsec تقدم نوعًا من التعقيد إلى DNS عندما لا يكون لديكم DNS موثوق أو لنقل مقاومة العملية، فمن الصعب الإضافة إلى اتصال DNSsec.

لذا، عند الانتقال إلى DNSsec-Africa.org، فسترون أننا نحتفظ بموقع إلكتروني. ولدينا أدوات تحاول يوميًا معرفة كيف يقوم cc في أفريقيا بعملهم ونحاول بناء سجل لذلك. لذا، نتحقق ونرى أول مرة نرى فيها مفتاح DNS لها، ونضع تاريخ. ونتبع أول مرة نرى فيها DS في منطقة الجذر لها. حسنًا. هذا ما سترون.

ولكننا نحافظ على تتبع التغير في المعرفات الرئيسية ونحافظ على تتبع الخوارزمية. حسناً؟ لذا، لدينا بالفعل cc جيدة في القارة الرئيسية، والتي وقعت حسب المنقطة. ولكن [غير مسموع]، فإن التوقيع أمر واحد فحسب. ولكن مع العمل، والذي يعني قبول DS عند تذكرها من أمناء السجل هو شيء آخر. لذا، من حيث عدد من يعمل، فهذه قصة مختلفة، وأعتقد أننا قريبًا سنسمع من الدكتور ليز عن، سنى، كيفية تقدم NA على سبيل المثال من حيث عدد سجلات DS لدينا منذ توقيع NA في 2009 وما إلى ذلك.

لذا، فلدينا ثلاثة cc حاليًا كمفتاح DNS، [غير مسموع] منطقة موقعة بدون تسجيل DS لمنطقة الجذر. والخطابات القادمة هي سيراليون. لذا، فنحن نراقب عن كثب. ولكن بالنسبة لعروض DNS نفسها، فما نقوم به هو أننا نزور الدول ولدينا فعالية لثلاثة أيام. واليوم الأول للتجمع. ونحن نطلب من المضيف دعوة كافة المشاركين لأن DNSsec لا تهتم فحسب بالتوقيع ولكن أيضًا بالتحقق.

لذا، نطلب من مضيفنا دعوة مزودي خدمات الإنترنت، كافة أصحاب المصلحة المهتمين بـ DNSsec، ثم نناقش. ونحن نعرض المصلحة، ما هي DNSsec، وبعدها إدراج

الأمور المحددة الآن. بعد ذلك، اليوم الثاني، لدينا يوم تقني، حيث نوضح للناس أنكم يمكنكم DNSsec، خاصة كيفية التحقق وما إلى ذلك.

وبعدها، اليوم الأخير، نجلس مع cc في القاعة، أليس كذلك؟ وبعدها، سننظر في عرض نظام السجل، أليس كذلك؟ ثم ننظر في كيف يمكننا نشر DNSsec، ونتوصل إلى خطة. حسناً؟ وسنحاول اتباع الخطة، إلا أن هذا ليس سهلاً. فما نكتشفه هو كثير من الوقت، نفس الأمر. تشغيل السجل غير موثوق وغير مستعد، أليس كذلك؟ ولا توجد أدوات مراقبة ولا يوجد فريق عامل كامل مخصص وما إليه، لذا فالأمر نفسه.

لذا، لقد انتهيتم إلى قول، "حسنًا. لنعمل على إصلاح السجل. حسناً؟" بعد ذلل، نضيف DNSsec، وماذا تقولون، ماذا سيكون عرضكم، حسنًا. هذه هو سبب أننا هناك، ونتمنى أن نتمكن من تحسين ذلك. كما يمكننا تحسين الاعتماد في افريقيا.

أعتقد أن الجميع سمع السنة الماضية بحادثتي DNSsec. والقول بمشاركة الناس، ودفعهم لاعتماد DNSsec، ولكن للأسف، السنة السابقة، لدينا اثنان من حوادث DNSsec. KE وفي نهاية السنة، لدينا حادثة أخرى، بوتسوانا.

كما أن الحادثتين يوضحان حاجتنا إلى العودة ومساعدة الناس في العمل حول كيفية إدارة الحادثة، استمرارية العمل، والتعافي من الكوارث. لذا، في ICANN، بعدها نضيف هذا الجانب إلى العرض، حسنًا؟ مساعدة الناس. وكانت لدينا مكالمة منذ بضعة أشهر مع cc لمناقشة خطة إدارة الدافع واستمرارية الأعمال وما إليه، لذا، سأتوقف هنا مارك. إذن هل يوجد أية أسئلة حول [غير مسموع].

مارك إلكينز: أعتقد أن ما نقوم به هو طرح الأسئلة حتى نهاية الجلسات الأربع، إذا كان لا بأس بهذا مع الناس. لذا، رجاء كتابة الأسئلة لوقت لاحق. شكرًا جزيلاً لك، ألين. أنا أعرف ألين منذ سنوات طويلة، وإذا كنتم ستذهبون إلى فعالية AFRINIC ولم يكن هناك، فهذه ليست الفعالية. شكرًا.

حسنًا. المتحدث التالي هو أنا. وسنتحدث وفق جدول الأعمال هنا. لذا، سأقدم موجزًا حول ما يحدث بالفعل في جنوب أفريقيا. جنوب إفريقيا. ونحن نقدم تدريب DNS لآخر عشر سنوات الآن، وحتى بعد ICANN في كيب تاون، فإن أول اجتماع ICANN لدينا في جنوب أفريقيا. وهذا يحدث مرتين سنويًا.

لذا، فهذه دورة تقديمية ومتقدمة في نفس الوقت، وهو ما يعني أن الأشخاص قد عرفوا ما هي DNSsec. وأعتقد أننا رأينا ثمار هذا. وبصورة شخصية، أنا أشغل DNSsec لسبع سنوات باستخدام نظام ISC DLV. فالرجاء عدم استبعاده. وقد كنت سأجيب على بعض أسئلتكم المطروحة حول ذلك في العرض من فيكتوريا، ولكني لم أفعل.

كذلك، لقد انتهيت من مشروع يسمي الاستبدال في العملية. ويجب أن نلاحظ أن أنظمة [Zeda EPP] لديها امتدادات DNSsec قد كنت أشارك وأطرح مفاتيح DS في مساحة اسم نطاق CO.za لآخر ثلاث سنوات. والسبب أن ZA هي الأكثر من الناحية السياسية من أي شيء آخر. والدليل على ذلك يتمثل في المدن الثلاث في gTLD، دربان وكيب تاون وجوبورج قد وقعت وهي تعمل بصورة جيدة.

لذلك، فالواقع أني نظرت في منطقة جوبورج مؤخرًا، ولديها بالفعل نطاق واحد موقع وقد حدث أنه الشخص الذي وضعه إما هنا أو هناك. لذا، كما قلت، كانت هناك ثمار من كافة هذه التدريبات. لذا، يمكنني أن أقول أن تلكوم جنوب أفريقيا، التي بقدر أنها ليست متوافقة مع أي شخص ويبدوا أنها تحاول بالفعل وتقوم بشيء ما بنفسها ولا تتحدث إلى المجتمع، فهني تأتي في الدورات التدريبية لأنها حرة. كما أنهم يشغلون جهات حل DNSsec والتي تصل إلى كما أعتقد حوالي 15% من الاستفسارات في جنوب أفريقيا. أو أن هناك 15% معلقة حول ذلك في عمليات البحث.

كذلك، أود أن أطالب بتوجيه الشكر الزيادة في جنوب أفريقيا، لأني لدي أندرو أوستين يجلس معي في آخر منتدى DNS في أفريقيا، ومعًا، وضعنا عملية التحقق من DNSsec في جهات الحل في ذلك الوقت. وأنا سعيد برؤية أن هناك نوع من الظهور بصورة لطيفة الآن.

لذا، يجب أن توقع جنوب أفريقيا أيضًا قريبًا. وهذا لن يحدث ببساطة. za. نفسها. كما قلت، يسهل هذا وضع الأمور في المنطقة، وتوجد هناك أغلبية المناطق. لذا، سيتضمن هذا كافة مناطق تشغيل ZACR مثل za. net COZA [غير مسموع] ،zaorg. .zalaw، .za

والمثير أن هناك بضعة نطاقات أخرى في جنوب أفريقيا، ولم يكن الجميع يعمل عبر مؤسسة مركزية في البداية، ولكنه موجه إلى أشخاص مختلفين للقيام بمستويات ثانية مختلفة. ولذلك يوجد بعض الارتباك.

لذا، أود شخصيًا النظر في edu.za وشخص آخر، صديق لي، ينظر في non.za. وقد وقع كلاهما ولديهما سجلات بجانب DLV. لذا، من الناحية التقنية، فهني هناك، بالرغم من عدد النطاقات الموقعة بالفعل، حسنًا، هذان نطاقات صغيران للغاية.

من وجهة النظر الأفريقية ووجهة نظري، فإن كافة العمليات المقابلة موجودة ومنذ مدة طويلة. لذا، لا يجب أن نرى أي شخص من أفريقيا يشتكي من أنهم لا يمكنهم قلب DNSsec هكذا.

وبعد ذلك تغيير الموضوع إلى حد ما. فقد وضعت ICANN طلب تقديم المشاريع لدراسة DNS في أفريقيا. كما أني متواجد في القاعة اليوم والسيد ويليام ستوك أيضًا في الأسفل هناك. كذلك، هناك مجموعة من 10-15 شخصًا آخر يقومون بنفس الدراسة أو يشاركون فيها.

تتضمن الدراسة النظر في سجلات DNSsec لمعرفة ما إذا تم التوقيع عليها. لذا، هذا ما يحدث. ولكن، إن كان سيكون هنا لأنكم من مدراء ccTLD في افريقيا أو المشتركين أو أمناء السجل فهذه الدراسة ستكون على بريدكم قريبًا. ورجاء مساعدتنا. يتعلق الأمر بالنظر واختيار الأرقام التي يمكن أن يقوم بها الأشخاص بنوع من التمثيل، أو تساعد بالتأكيد في وجهة النظر المستقبلية.

وأعتقد أنني سأترك هذا ينتهي. فهو يكفي. عضو اللجنة الثالث هذا الصباح. عضو اللجنة الثالث هذا الصباح هو سارة.

سارة مونتيرو: نعم.

مارك إلكينز: وقد قدمت بالفعل سيرة ذاتية في النهاية، أليس كذلك؟ درجة علمية في علوم الكمبيوتر من جامعة لشبونة. إنها برتغالية. وعضو في فريق البنية التحتية في DNS، منذ 2006. كما أنها تتولى مسؤولية إدارة ccTLD في البرتغال، وقامت بأدوار متعددة في المجال التقني في القيام بمختلف الأمور، وستظهر هذه الأنشطة ضمن امتدادات DNSsec المدرجة هنا.

هل ستتحدثين الإنجليزية؟

سارة مونتيرو: نعم.

مارك إلكينز: أوه، حسنًا. شكرًا لك، سارة. الميكروفون لك.

سارة مونتيرو: طاب صباحكم جميعًا. كما قال مارك، أنا عضو في ccTLD، .pt وأنا في الفريق الفني لكن اليوم، أنا هنا نيابة عن بعض نطاقات ccTLD الأفريقية حيث أن pt DNS. معينًا كجهة اتصال فنية في IANA. الشريحة التالية، من فضلك.

لذا، قبل أن أبدأ الحديث بصورة خاصة عن بعض نطاقات ccTLD، أريد فقط أن أخبركم عن LusNIC، وهي منظمة ccTLD باللغة البرتغالية تم إنشاؤها السنة السابقة. لذا، فمهمتها تتمثل في الارتقاء والتعاون في الدفاع عن نطاقات ccTLD باللغة البرتغالية. كذلك، نعتقد أنه بهذه المنظمة، سنتمكن من مساعدة بعض نطاقات ccTLD خاصة في أفريقيا ونطاقات ccTLD الأخرى. لذا، فالدور الرئيسي هو المساعدة والتعاون بين كافة نطاقات ccTLD. الشريحة التالية من فضلك.

لذا، في LusNIC، كما قلت، يتمثل الغرض الرئيسي في مشاركة المعرفة في مجالات التدخل فيما يتعلق بالأمور الفنية والأمنية والقانونية والممارسات الجيدة. وتتمثل الرسالة في تصور الإجراءات المشتركة والتقدم في النمو المستدام لنطاقات المستوى الأعلى باللغة البرتغالية، خاصة br. من البرازيل وcv. للرأس الأخضر وgw. لغينيا بيساو وpt. للبرتغال وst. لسانت تومي وبرينسبي وao. لأنجولا.

لذا، الآن، هناك تلك الموقعة والأعضاء في المنظمة. ولكننا نتطلع لأعضاء جدد ومشاركة كافة هذه الخبرات. الشريحة التالية من فضلك.

لذا، بصورة خاصة ao. من أنجولا. ونظرًا لنجاح DNS .pt في [غير مسموع] في إدارة نطاق المستوى الأعلى للبرتغال في 2013. لذلك، ستنجح أيضًا في المسؤوليات الأخرى. لذا، فنحن نساعد ao. من أنجولا. كما أننا في نهاية 2015، كان لدينا 364 من أسماء النطاقات المسجلة. وبالنسبة لشؤون DNSsec، فقد عقدنا تدريبًا لمدة أسبوع، تدريب DNS، حيث نحاول مشاركة معرفتنا في أمور DNS في لشبونة على موقع DNS .pt الخاص بنا.

لذا، فقد اقترحنا تحسين المعرفة بكل من DNS وDNSsec. كما قدمنا لهم ورشة عمل علمية وكان لدينا ستة مشاركين من جهتين مختلفتين. الشريحة التالية من فضلك.

بخصوص cv.، الرأس الأخضر. في 2010، تمكنت DNS .pt، التي أدارتها بالأساس من cv. [غير مسموع] من نقل الأدوار والمسؤوليات الأخرى إلى ANAC، الهيئة الوطنية للاتصالات، وقد بدأ توليهم لهذا الدور بصورة مستقلة.

لذا، في نفس السنة، استضفنا ورشة عمل للجهات المحلية حيث كنا نحاول الترويج لنطاق المستوى الأعلى cc. وفي 2013، مرة أخرى، عقدنا تدريب عملي في الموقع حيث دعونا الفريق الفني في ANAC. كما حللنا كافة البنية التحتية في CV، وأنشأنا تقريرًا لمساعدتهم في تكوين كافة التعديلات اللازمة لاعتماد DNSsec. لذا، أعتقد أنهم مستعدون لاعتماد ذلك. ولا أعرف لماذا لم يقوموا به، لكني أعتقد أنهم يشعرون بمزيد من الراحة إذا ساعدناهم، لذا، فهم يحاولون ترتيب تاريخ لموعد قدوم البرتغال مرة أخرى لمتابعة النشر أو ربما سيكونون هناك لمساعدتهم، لذا لا أعرف. إذن إننا نتقدم للأمام.

كذلك، لقد عرضنًا أيضًا في هذا الشأن وركبنا خادم الاسم في منشآت ANAC كما قلت لمساعدتهم في الإدارة الفنية في ccTLD بنفسهم. كما قدمنا أيضًا حقوق نظام الإدارة السابق لدينا في pt. والبرامج بهدف مساعدتهم في إدارة النظام بأقصى قدر من الاستقلال. الشريحة التالية من فضلك.

والأخيرة، إنها gw. لغينيا بيساو. في يوليو 2014، كان RN لدينا مسؤولاً عن مراقبة gw. ويعود نطاق المستوى الأعلى من IANA والتسجيل والإدارة [غير مسموع] إلى منطقة غينيا بيساو. لذا، الآن، يتولى pt. DNS المسؤولية عن العمليات الفنية والإدارية والإدارة القانونية لسجل أسماء النطاقات وgw. من خلال طلب IRN. مع ذلك، نتطلع لنقل كافة هذه الأدوار إلى الجهة المعنية. ولكننا سنتمكن من القيام بذلك بعد تدريب مكثف وإعداد للشبكة المناسبة والبنى التحتية الفنية [غير مسموع]. والشريحة التالية، من فضلك.

حسنًا. يمكننا أن نشارك معكم أنه في التحليل التراكمي بين البيانات، إنه التحقق، وقد وصلت .gw في نهاية عام 2015 إلى 2200 اسم نطاق. لذلك، نعتقد أن هذا التطور كان ممكنًا لأن NSPT تمكنت من الاعتماد على السجلات البرتغالية لاحتضان ccTLD الجديد في أعمالهم. كما شارك أيضًا بعض المشتركين الدوليين. وكرقم إجمالي حتى الآن، كافة أمناء السجل الخمسة عشر. الشريحة التالية.

بخصوص DNSsec، في فبراير 2015، حيث أننا ندير المنطقة بالكامل، فقد سجلنا في DNSsec. ولا نزال نقدم سجل DNS في منطقة الجذر حسب الأمور السياسية، لكنه أمر متعلق بالوقت.

وفي مايو من نفس السنة، مرة أخرى، استضفنا ورشة العمل. وهذه المرة، ذهبنا إلى غينيا بيساو، ومع تقديم نظرة عامة على الإنترنت، خاصة بشأن أمور DNS، والأمن الإلكتروني وأمور DNSsec، فقد تمكنا من تقديم عرض لإجمالي 42 مشاركًا. لذا، أعتقد أن هذه هي كافة المعلومات التي حصلنا عليها، لذا، أتمنى أن تكون مفيدة، وشكرًا لكم.

مارك إلكينز: شكرًا جزيلاً لك، سارة. ولم أدرك أن هناك هذا القدر من الدول المتحدثة بالبرتغالية في أفريقيا. ولكنكم الآن تضعونه هناك، أفهم، نعم. والمتحدث الأخير هذا الصباح من اللجنة، اليد الذي أعرفه لمدة طويلة للغاية، الدكتور ليز إبرهارد.

ولديه معرفة وساعة بهذا المجتمع منذ اليوم التقني. كما أنه سيفسد شيئًا ما الآن. فحيلته المفضل في ICANN هي سؤال الناس عن مهنتهم، والمهنة النهارية، لأنه ليس لديه أي شيء ليفعله مع تشغيل سجل ccTLD. فهو طبيب نساء.

مع ذلك، فللحديث بجدية، إنه شخص مولع من وجهة نظري الشخصية بالقيام بالأمور المماثلة لحماية النساء والأطفال في ناميبيا. وهي بالفعل تغير القانون وتسهل للنساء أن تعامل كالنساء في ناميبيا. لذا، فلديه قلب طيب في مكان ما. ولا ترون ذلك، لكنه لديه بالتأكيد قلب طيب في مكان ما.

على أي حال، الرجاء المتابعة. لا، وارين، لم نضحك عليك عند دخولك، حسنًا، بعضنا كان كذلك، ولكن الغالبية لا.

إيبرهارد ليسه: أوه، لقد بدأت. أوه. أقول دائمًا أني اعتدت على وجود مهمة نهارية، وهي طبي نساء، وبعدها، قلت أيضًا أن لدي مهمة بالليل، وهي طبيب توليد، ولكن نظرًا لبعض الحقائق المتعلقة بأن التأمين على التقصير وصل إلينا، فليس علي القيام بهذا بعد الآن، حتى أتمكن من النوم.

ولكن علمتني هذه المهنة بضعة أمور، على سبيل المثال، هل يمكنك الانتقال للشريحة التالية؟ أن المريض لا يهتم بالفعل، بعدد الزيارات إلى الطبيب، ولكن ما إذا يمكنني حل المشكلة. وأنا أفكر بشدة في بضعة أمور. فأنا سعيد للغاية برؤية أن [غير مسموع] الدول الأجنبية قد اعتمدت من قبل الرئيس السابق للمساعدة في القليل، ولكني أعتقد أنه أسلوب خاطئ على المدى الطويل، وهو الأسلوب الخاطئ على المدى القصير أيضًا.

في DNS، لم أتمكن من اكتشاف ما تنفقه العروض من المال، وكنت أتمنى أن يقال هذا في العرض، ولكني سأبحث ذلك مع خافيير، المدير المالي. وقد اعتاد على رسائل الآن.

هذا ما يفترض أن يكون الأمر، فسيكون عرض DNS [غير مسموع] الكثير ومن المفترض أن يدعم اعتماد DNSsec. ولكن إن أمكنني عرض الشريحة التالية، كما نرى في 2013، أنها كانت صورة هناك، والآن يمكن عرض الصورة التالية.

لم يتغير أي شيء بالفعل، لذا، فنحن نضيع الكثير من النقود في السفر على الدرجة التجارية ونقوم بورش عمل لطيفة وننظر فيما نعرفه جميعا أن مدراء ccTLD كسولين للغاية بالأساس فيما يتعلق بأداء وظائفهم. وبوضوح، إن لم يمكنهم القيام بالمهمة الرئيسية، فلن يكتشفوا شيئًا يمكن لطبيب نساء بسيط القيام به خلال ستة أسابيع عند كان مريضًا بعد جراحة في 2009. ليست BIND بهذه الصعوبة.

فمن المشين أن تعمل دولتان فحسب، وهذه تنزانيا وربما الست الأخرى غير مرئية جميعًا لأنها جزر صغيرة وتعمل على منصات أخرى. وفي حالة تشغيل جزيرة صغيرة لمنصة org.، فهذا لا يحسب. كذلك، عندما كانت غينيا بيساو ccTLD تعمل على pt.، فهذا لا يحسب. والأمر بديهي، وليس علم صخور، فلا تهتم أن لدينا الموارد البشرية لدينا. ونحن نرسل الأشخاص إلى الجامعات للحصول على درجة الماجستير في علوم الكمبيوتر لكننا لم نتمكن ببساطة من القيام بأمور بسيطة مثل هذا. الشريحة التالية، من فضلك.

بالأساس في الوقت الراهن، وأنا سعيد أني يمكنني أن أسأل الأشخاص من .cz عدم بدء اللهاث من الآن. فسنمضي إلى هذا. وهذه مزحة. توجد طريقتان، عندما كتبت هذا العرض، كانت هناك طريقتين لتنفيذ DNSsec. وDNSsec بسيطة لكنها ليست سهلة.

وما نريد على الجانب الآخر هو أن تقدم لنا [Tarlis] الأجهزة الرخيصة نسبيًا. نعم؟ ونحتاج ثلاثة منها. فكل نطاق ccTLD يحتاج ثلاثة منها، وأسمع لحسن الحظ أنكم يمكنكم تغيير البطارية في [Tarlis]، لذا ليس عليكم استبدالها طوال الوقت. ولكننا نحتاج إليها بسعر معقول.

لذا، ما نحتاج بالفعل للنظر فيه هو شيء يمكننا القيام به مقابل 20 دولارًا. أحد الإجابات هي برامج HSM كما أن BIND يمكنهما ببساطة القيام بهذا، وإذا كانت BIND، فمن السهل بالقيام بذلك في البرامج إلا أنها لا تدعم HSM بعشرين دولارًا على الأقل ليس

خارج الصندوق. كتب [غير مسموع] دفعة، ولكن المشكلة أنه عند تحديث BIND، سيكون عليكم إعادة تقديم الطلب، وهذا ليس مناسبًا ولا يمكن القيام به.

إذا حدث أني أمكنني فقط التحديث مع مدير الحزمة وسينجح هذا، فسأتولى البحث عن الأخطاء التي تريدون، وسيتم إنجاز هذا.

كذلك، من الصعب إعداد OpenDNSSEC. ومن الصعب تصحيح الأخطاء فيه. كما أنه يدعم برنامج HSM، لكنه على Ubuntu، هذه البطاقة تتطلب مكتبة، وهذه المكتبة لديها عادة سيئة تختضر لكنها موجودة. لذا، فلدى OpenDNSSEC عادة سيئة بإنهاء العمل، وانتهاء التسجيل بدون إخطارك. لذا، فهذه ليست طريقة بسيطة للقيام بهذا. هل لنا بالحصول على الشريحة التالية، رجاءً؟

شاركت OpenDNSSEC في العديد من المشكلات في نطاقات ccTLD بصورة أو بأخرى. ومن الصعب تصحيح الأخطاء فيه. فما أقوم به هو تسجيل lisse.na في بطاقة HSM البرامج. وعلى أيضًا إنهاء البرنامج الخفي [غير مسموع] ثلاث أو أربع مرات يوميًا حتى يبدأ العمل مرة أخرى وبعدها أعيد التسجيل خلال يوم أو ما شابه، إلا أنه ليست طريقة جيدة لتشغيل خط.

لذا، عندما كتبت هذا العرض، كنت أفكر في أننا علينا، بدلاً من تضييع مزيد من النقود في السفر في عروض السفر من DNSsec، ولكن أخذ الأموال والنظر فيما يفيد مثل التسجيل الإضافي في DNSsec، وصياغة برامج مستقلة يمكنكم تشغيلها على سطر الأوامر. وسيكون هذا أسهل في الإصلاح. وبمجرد تعليق هذا، يمكنك وضعه في تعليمات برمجية شاملة وتشغيله على [غير مسموع] وسيعمل. وهذه هي التكلفة المفترضة. هل لنا بالحصول على الشريحة التالية، رجاءً؟

في نفس الوقت، ذكر أندري [غير مسموع]، الذي تحدث في اليوم التقني يوم الاثنين، على الغداء أنها لم تكن DNS، الملتزمة بالمسؤولية عن العالم، ويمكن الحديث بالفعل عن بطاقة HSM البرمجية هذه. لذا، سأعمل معهم على معرفة أننا يمكننا العثور على طرق تعمل على Ubuntu خارج الصندوق، فحتى إذا كان هناك [غير مسموع] خاص للطريقة التي يمكن بها القيام بالتحديثات حول مدير المجموعة، وإن نجح هذا، فربما

تكون طريقة يمكننا من خلالها الحصول على حل معتمد على الأجهزة، مما يتسبب في زيادة الأمن ولا نضطر لاستخدام هذه الآلة باهظة الثمن.

إنها مجرد بطاقة صغيرة. فهي رقاقة صغيرة تكلف 20 دولارًا، تشتريها، وتكلفتها 20 يورو، ويمكنها شراؤها في ألمانيا، وإذا اشتريتم خمسة من دول نامية، فسيتاح لكم ستة بنفس السعر. فبها رقاقة صغيرة، تقوم بالفعل بالتسجيل في الرقاقة. كما يمكنها القيام بخمس عمليات تسجيل كل ثانية.

هل يمكنني الانتهاء من العرض رجاءً؟ أنطوني [غير مسموع] شخص لا أراه عزيز للغاية على قلبي، وهو يعرف هذا، أتاح نفسه مؤخرًا للتوظيف النهائي ونشر على الموقع الإلكتروني أنه تم فصله، وقال بالأساس لأن السوق [غير مسموع] يكون به خمس أنواع من السجلات. فلا يرد اثنان علينا بالفعل، وبترتيب تنازلي، يكون أسلوب المتجر الكبير هو ما تحاول بعض ccTLD القيام به في بيع كمية كبيرة من النطاقات بربح ضئيل.

هل ينجح هذا، أنا لا أعتقد ذلك. تود ICANN أن يكون السجل وظيفة فنية فحسب مهتمة بالبنية التحتية ومستوى الخدمة، وما تعمل عليه لنا هو أعمال صغيرة، مع الحفاظ على انخفاض التكلفة وبناء الأعمال مع الوقت والنظر في إيرادات جيدة أو مستمرة. كما نقول بالأساس أننا نريد معدل تجديد مرتفع وما أراه والشريحة التالية، هذا ما علينا أن نجده في الشريحة التالية.

باختصار، فإن الأجهزة باهظة للغاية إذا دفعنا 20 ألف أو 30 ألف يورو لجهاز واحد، فهذا ببساط خارج المتاح. ولا يمكننا القيام بهذا. فلا تزال HSM البرمجية غير مستعدة للوقت الرئيسي. وأحد الأمور التي يسهل للغاية القيام بها ولا أفهم سبب عدم استخدام العديد من ccTLD لها هو إعداد طريقة آمنة لدفع المنطقة نحو PCH. فهي تسجل بأسلوب آمن للغاية بالفعل وتدفع الأمر بالكامل لك أو تتصرف كأحد خوادم الاسم للسلطات حيث أنهم لنا، ونحن نقوم بهذا لنطاقات المستوى الثاني بالفعل.

كذلك، قبول أدوات [غير مسموع] سجلات DNS، والتي تتمتع باستخدام واسع في أفريقيا، نسخة لاحقة، كل شيء من المنتصف إلى آخر سنة متوقعة لسجل DNS.

وبالنسبة لسجلات DS كنا نتعامل أنا ومارك مع هذا. ولم آتي هنا بالفعل لعرض عدد العملاء الذين لدينا. فمن المفترض أن لدينا عملاء سيتولون هذا.

وإذا ذهبنا غلى البنك وحاولنا توضيح [غير مسموع]، حسنًا، ولكن لدينا https يعمل لنا. لا يهم، فهم دائمًا ينسون تجديد الشهادة ويمكنني أن أضمن أن ستاندرد بنك في 22 من ديسمبر هذه السنة سيفشل لأن الشهادات ستنتهي صلاحيتها.

كذلك، تم إنشاء رسالة العودة وسيأتون. وإن أمكننا بناء نظام رخيص نسبيًا، وهذه هي الوظيفة. ففي النهاية سيبدأ العملاء في اكتشاف هذا. وتريد الحكومة تفويض DNSsec. كما أخبرناهم بعدم القيام بهذا فقط حتى يمكننا التدقيق من ألعى لأسفل عبر الأجهزة.

ولا أعتقد بالفعل أنها مشكلة عويصة أن يتم تسجيلهم. كذلك، إذا أخبرت أمناء السجل لدي، الذي يمثلون أيضًا مزودي خدمات اتصال، إذا لم نضع جهات حل معتمدة، سنقدم لكم أُقساط صغيرة على التسجيلات أو خصم، إن قمتم بهذا، فسيشرعون في القيام بهذا بسرعة إذا أصبح الأمر تجاريًا.

وأرى أن هذه الشريحة الأخيرة. شكرًا جزيلاً لكم.

مارك إلكينز: شكرًا جزيلاً لكم. لديه بالفعل قلب في مكان ما. حسنًا. لدينا حوالي عشر دقائق من الأسئلة. ومجرد تعريف سريع. إذا نظرنا فيما هي وحدات HSM، ومال إلى ذلك، فهي وحدة أمن الأجهزة. وبالنسبة لي، هناك HSM برمجية والتي ستكون جزءًا من برنامج قام بصياغته ريتشارد بلكين من السويد. حسنًا.

شخص غير محدد: نعم. كجزء من مشروع DNSsec، بالفعل، ولكن تم صيانته [غير مسموع] ممولاً من ServNet بصورة كريمة.

مارك إلكينز: حسنًا. كنت أمر بسرعة على التعريفات. ويتمثل موضوع HSM الذي كان إبرهارد يتحدث معي حوله في أنه يبدو كبطاقة ائتمان مع بطاقة ذكية ووحدة ذهبية صغيرة. نعم، إذن PKC [غير مسموع]. والأمر اللطيف حول ذلك هو أنها بالفعل رخيصة، وهي بالفعل رخيصة، كما أنها متميزة في التكوين المسبق لمجموعة كاملة من التوقيعات والأمور، وبعد ذلك، على الجانب الآخر، لديكم HSM مثل السجلات والأجهزة الإلكترونية والجذر مسجلة، ويمكن أن تأتي في مجموعات ضخمة.

لذا توجد ثلاثة أنواع من وجهة نظري. هل تريدون توضيح ذلك، أم نترك دان؟ حسنًا. لقد كنت سأطرح سؤالاً سريعًا أولاً للتمهيد، ولكن يبدو أنه سيحدث. آلين. 54 دولة في افريقيا. ما عدد الذين لا يزال عليهم القيام بهذا وما طول المدة المستغرقة كما ترى؟

آلين إينا: ما نقوم به هو إعادة البيع للأشخاص ونحن نزور بالفعل من يريد منا القدوم بالفعل. لذا، فنحن لا نذهب فحسب. نحن [غير مسموع]، وقد بعنا ونناقش وسنرى موضع الأشخاص، ونرى ما إذا كانت لديهم رغبة في استضافة فعالية. لذا، فالأمر لا يتعلق بالانتقال إلى الأماكن. نحن لا نزور كل ccTLD، لذا، فهذا كل ما يمكنني أن أقوله حول العدد لأني لا أعرف الآن متى تأتي المرة القادمة. لذا، يعتمد الأمر على الأشخاص المستعدين ومن يريد الاستضافة.

مارك إلكينز: كان هذا بالفعل سؤالي لألين. لذا، إذا كانت هناك دول في القاعة من أجزاء أخرى ويودون طرح العرض للعمل مع ذلك. ولدي بالفعل تعليقات رائعة من الآخرين حول ما قاموا به في هذه المجالات. كيف يمكننا التوجه نحو فعل هذا؟

آلين إينا: طريقتان، الحديث إلى أو إلى بيير أو إلى هيئة أفريقيا في ICANN، أو حتى مجتمع الإنترنت، أو الحديث إلى الأفراد في ICANN DNS مثل [غير مسموع]. وتستخدمون مختلف الطرق لنفس [غير مسموع].

مارك إلكينز: حسنًا. سأقول فقط أني أعتقد أن ذلك رائع أن تضيفوا جزءًا حول التعافي من الكوارث والاستعداد. وهو أمر مميز. لذا، بينما معي الميكروفون للحظة، سأشجع الجميع فحسب على الانضمام إلى دراسة DNS التي تحدث عنها مارك. ونحتاج، كما ترون في البداية عندما تحدثنا عن المقاييس والأمور، إلى مزيد من البيانات حول الاستخدام والتوظيف وكل هذه الأمور. لذا، رجاءً المساعدة في هذه الدراسة عند ظهورها.

جولي هيدلوند: أنا أشير إلى ذلك فحسب. والرجاء عدم ذكر الاسم والانتماء. كما نحتاج ذلك أيضًا من الزملاء المشاركين معنا عن بعد. وأعرف بعضكم، لذا فنحن نضع هذا في الدردشة، ولكني لا أعرف الجميع. وكذلك، إن كان لديكم أي سؤال وأنتم غير موجودين على الميكروفون، فكاثي شنيت هنا ستتحرك مشكورة بالميكروفون. لذا، تأكدوا من طرح الأسئلة بالميكروفون وإلا لن يتمكن الزملاء المشاركين عن بعض من سماعكم.

وبعد ذلك، فقط للإشارة، مارك، لدي سؤال في الدردشة، إن أمكن إضافته إلى قائمة الانتظار.

مارك إلكينز: لا أرى أية أسئلة في الوقت الراهن. هل تود قراءة هذا السؤال؟ عذرًا. فكتوريا.

فيكي ريسك: ولدي تعليق واحد. إبرهارد، أعرف أنك تنظر في الدعم لبطاقات الائتمان هذه في HSM البرمجية وإذا أرد ريك تقديم مجموعة، طالما أن لدينا اختبار لذلك وقليل من الوثائق، فسيسعدنا إتاحتها بصورة اكبر لمستخدمي BIND الآخرين. وهذا بالطبع ما ينجح كمصدر مفتوح. لذا، في الواقع، حتى إن أردت تقديم عرض إلى الزملاء الآخرين المهتمين باستخدام HSM فيسعدني تمويل ندوة عبر الويب أو شيء من هذا القبيل.

إيبرهارد ليسه: لذلك اسمحوا لي قول ذلك فقط. هل يوجد تغيير في رؤية ISC بهذا الصدد؟ لأني كانت لدي مراسلات سابقة مع جهة التنفيذ. ولم يكن مهتمًا.

فيكي ريسك: لدينا خبير تشفير ولديه رأي مختلط حول قابلية اعتماد FIPS لبطاقة HSM وما إلى ذلك. هناك فرق كبير بين التوصية بحل على أنه قمة التميز في التشفير وتمكين الناس الذين يحاولون تشغيل DNSsec. وأنا متأكد من أننا يمكننا التوصل إلى حل وسط كما لو كان لديكم على وجه التحديد مجموعة عمل، بالتأكيد.

إيبرهارد ليسه: لذا فإن هذه أخبار طيبة. وسأجتمع مع ريك ونتواصل معكم ونرى ما يمكننا القيام به.

مارك إلكينز: أسمع هذا كدعوة للاجتماع. لقد كتبت هذا بالفعل إلى فكتوريا حتى تدرج ISC نوعًا من الدعم القياسي لبرامج HSM على البطاقة. هل يمكن طرح السؤال عن بعد رجاءً؟

جولي هيدلوند: شكرًا لك، مارك. السؤال عن بعد من ماركوس من Global Village. وسؤال هو "هل السجلات الأفريقية تستخدم امتداد EPP DNSsec قياسي، أو ستستخدم نمط .pt في اختيار سجل DNSsec؟"

سارة مونتيرو: أعتقد أن السؤال لي. لذا، فيما يتعلق بالسجلات الأفريقية، فهذا ما تساعد فيه DNS PT. وليس لديهم امتدادات EPP منفذة حتى الآن، ولكني أعتقد أن DNS PT لن تنفذ نفس الأساليب التي تسري على pt. لأننا لا نحاول نسخ ما يقوم به الآخرين، بل نساعدهم فقط في إعداد نظامهم ونحاول عبر المعرفة والمتخصصين الفنيين لديهم تحسين ما لديهم حتى نتمكن من القيام بالأمر.

لذا، بالنسبة للوقت الراهن، يمكن أن تقدموا معلومات DNSsec في نص بسيط أو شيء من هذا القبيل، ولكن في المستقبل أعتقد أنهم سيقررون أنه ليس pt. بالتأكيد. لذا لا أعرف.

مارك إلكينز: يمكن لأي سجل ccTLD أو gTLD يستخدم أدوات [غير مسموع] من إصدار أحدث من يونيو أو مايو 2015 أن يقبل سجلات DS من خلال EPP قياسي. وهي تعمل خارج الصندوق لأي أمين سجل معتمد من ICANN. كذلك، يمكنهم بالطبع وضعها في GUI أو يمكنهم إرسالها عبر البريد الإلكتروني، ولكن بالنسبة لي أنا ومارك، فكانت لدينا مشكلة، لم نستطع حلها. وفي النهاية، تم إصلاح المشكلة والآن تعمل في الحالة القياسية.

مارك إلكينز: السؤال التالي.

روبرت مارتن ليجين: روبرت من PCH. لا، لقد كنت فقط أعلق على ما قاله إبرهارد وعرضه حول تسجيل PCH لنطاقات TLD. فسيسعد PCH أن تأخذ النطاقات وتوقعها مجانًا، وتسلمها إلى [غير مسموع]. ولا تحتاجون للذهاب إلى أي خدمات أخرى لدينا، ولكننا نرحب للغاية بكم بالطبع. كذلك، إن كنتم تريدون Anycast أو DNSsec أو مهما يكن، سيسعدنا بالحديث معكم.

روس موندي: حسنًا، أود أن أشكر اللجنة على المجموعة النهائية من العروض. وأنا روس موندي من SSAC. ويسعدني للغاية أن أرى مقدار التقدم المحقق في هذه القارة عبر السنوات الخمس السابقة، وبالأساس، لقد كان ضخمًا. كذلك، أحد الأمور التي وجدتها مثيرة للغاية في مجموعة العروض هي أنه عندما ذكر إبرهارد أن الحكومة كانت تفكر في تفويض استخدام DNSSEC، وهو ما يعتبر في حد ذاته تقدمًا إيجابيا بأن أحد الحكومات تفكر في القيام بهذا.

ولدي بالفعل سؤالان. اولاً، هل هناك حكومات أخرى في أفريقيا تفكر في اتخاذ خطوة مماثلة؟ والتفويض، لقطاع أو جزء من المجتمع، باستخدام DNSsec. ثانيًا، لدي سؤال مستقل إلى حد ما، هل لا تزال وظيفة أمين السجل تواجه تحديات كبيرة فيما يتعلق بعمل DNSsec بالصورة المناسبة في أفريقيا بالكامل؟

إيبرهارد ليسه: يمكن أن يقدم المشترك فقط سجلات DS، إن أمكنك استخدام أدوات [غير مسموع]، فإن الطريقة الثالثة متاحة مع واجهة المستخدم الرسومية. ولكن لا يوجد طلب. كما يمكنكم الذهاب إلى البنك وتوضيح أنها تعمل، وسيقولون لكم "لا، لقد حصلنا على شهادات SSL وهي جيدة، كما أنها تحمي المستخدمين." فهم لا يفهمون فحسب. ويمكنكم توضيح ذلك 1000 مرة، كما يمكنكم توضيحه بأدب شديد، والقيام به بسهولة، والقيام به بتعقيد أكبر. بالطبع. فهم يطورون تطبيقات لطيفة. وتطبيق الخدمات المصرفية من أحد البنوك الأصعب هو الأفضل الذي رأيته في العالم، ولكنهم فقط غير مهتمين.

وأنا أعتقد بقوة أنكم ليس عليكم دفع الطلب من جانب البائع. فنحن نقدم الخدمة، ونقوم بإنشائها. وإذا أرادوا القدوم لنا، فسيأتون. وإن لم يريدوا، فلن يأتوا. نحن نخبر الحكومة أن عليهم تفويض أي م من الجهات التي يجب التحقق منها.

مارك إلكينز: شكرًا لك، إيبرهارد. أنا أنظر إلى الساعة هناك فحسب. وأرى أيضًا أن AFRINIC تستخدم موقع SSL لتحميل سجلات DS، وهذا يعمل بصورة جيدة. دان، لديك سؤال.

دان يورك: بسرعة لسارة. أنا أكره روبرت بالفعل. أريد الحديث إليها. نقطة. أريد الحديث إليها. لذا، أولاً، أود أن أوجه الشكر فحسب إلى سارة على القدوم والحديث عما تقوم به LusNIC. وأشارك مارك، لم أكن أعلم أن هناك العديد من الدول المتحدثة بالبرتغالية في أفريقيا حتى آخر مرة عرضت هذا، وهو ما كان مفاجئًا لي. لذا، شكرًا على لاقيام بهذا، ورجاء الاستمرار.

سؤال واحد فحسب. لقد ذكرتي في gw.، أنهم سجلوا، وهم جاهزون للبدء، ولكن هل التأخيرات بسبب سياسي أو مجرد تأخير في هذه المساحة، أو هل يمكنك الحديث قليلاً عن هذا أو ما شابه؟

سارة مونتيرو: لقد بدأت بالتأخيرات التقنية وحيث أننا نحتاج، عند تقديم المعلومات في IANA، إلى وجود موافقة الجميع، وهي ليست سهلة الاستخدام للأشخاص التي لم يستخدموها فحسب. أعتقد هذا، ولا أعرف. ولكن المشكلة، ليست مشكلة، ولكن pt. في 2015 شدت أيضًا تحولاً من البنية التحتية القديمة إلى بنية جديدة. لذا، أيضًا، ستتغير خوادم الاسم التي تتضمن تفويضات بالفعل، لذا، فنحن نحاول القيام بنفس التغيير في الحال، وهذه الطريقة، ستكون أسهل للجميع لجهات الإدارة والأمور الفنية.

لكننا نعمل بجد على هذا، ونعتقد أنه في 2016، سنتمكن من القيام بهذا.

دان يورك: حسنًا، شكرًا. شكرًا.

مارك إلكينز: سؤال أخير، [غير مسموع].

شخص غير محدد: أود الإضافة إلى ما قالته فيكي. فقد نفذنا ذلك لبدء دعم [غير مسموع] CS في DNS ونحن الآن نجرب مختلف HSM. لذا، إن كانت لديكم HSM، تودون إضافتها إلى منتجاتنا، فنود، إن كان يمكنكم تقديم وصول عن بعد إليها لاختبارها، وسيسعدنا وجود الدعم في هذا الصدد، لأنه في حالة تنفيذ دعم CS-11 [غير مسموع]، فذلك لا يعني أنها تدعم كافة الوحدات. فكل منها مختلفة للأسف.

مارك إلكينز: شكرًا جزيلاً لكم. وتاليس، رجاءً. باختصار. 30 ثانية لكل شخص. آلين.

آلين إينا: نعم. أود أن أتمكن من السفر على درجة رجال الأعمال ولكننا نسافر في مؤتمرات العمال لعروض DNSsec وجزء من العرض هو أيضًا توفير بعض الموارد. لذا، إن كنتم ستنتقلون إلى موقع الويب، فترون أن لدينا مواد، ومن ثم، أشخاص. وأعتقد أن العروض لا تنظر بالفعل في الجانب الفني كما قالت ليز، فنحن نحتاج أيضًا لمشاركة المجتمع لتحقيق الحاجة لأفراد متابعين.

بخلاف ذلك، فإن السجل الذي سجلتم مملوك، ولكن لا أحد يتابع، لذا [غير مسموع].

مارك إلكينز: شكرًا. انتهت فترة 30 ثانية.

آلين إينا: شكرًا.

مارك إلكينز: أنا سارة.

سارة مونتيرو: عذرًا.

مارك إلكينز: باختصار، لديك 30 ثانية.

سارة مونتيرو: حسنًا. أعتقد أن الهدف الرئيسي هو مساعدة DNSsec في الانتشار في كل دولة وكل نطاق ccTLD وgTLD. حسنًا، نحاول القيام بذلك. ونحن نشارك فقط كافة المعرفة ونبذل قصارى الجهد، ونتمنى أن نتمكن من مساعدة الجميع.

مارك إلكينز: شكرًا جزيلاً لكم. دكتور.

إيبرهارد ليسه: أجل. الآن، يمكنني العدد حتى 29 ثانية لأني ليس لدي موجز جيد بالفعل. وما أراه أننا كأفريقيين كسولين بطبعنا ونود -- نعم، أنا كذلك. حتى إن لم تعتقدوا أني كذلك. وكذلك مارك. والنقطة هي أني لا أعتقد أن القيام بهذا من القيادة للقاعدة سيساعد، وإنشاء طلب مصطنع لن يساعد أيضًا. فعلينا أن نقدم الموارد المتوفرة ولكن النتيجة ستكون متابعة النظام من القاعدة للقيادة. كما أن علينا بالأساس عدم إقناع أي شخص بالقيام بهذا. فإن أرادوا القيام به، فسيقومون به، وبالتالي سينجح. ويجب علينا توفير الموارد عمليًا، وليس فقط من خلال الحاجة للذهاب للاجتماعات.

مارك إلكينز: شكرًا جزيلاً لكم. شكرًا للجنة. عرض رائع. وتصفيق.

جولي هيدلوند: شكرًا لك أيضًا مارك. شكرًا جزيلاً لك. إشراف رائع.

مارك إلكينز: ونحن نتطلع إلى رؤية هذه الخريطة مملوءة المرة القادمة التي نأتي فيها إلى أفريقيا.

جولي هيدلوند: لذا، من المفترض أن نحصل على استراحة. ونحن على علم أننا سنعود بعد 15 دقيقة، وأعتقد أننا يمكن أن يكفينا هذا الوقت. ما رأيك، دان؟

دان يورك: بالتأكيد. أعني، ما هي الاستراحات؟ ماذا لدينا هنا؟

جولي هيدلوند: عذرًا.

دان يورك: أجل. أنا أتأخر عن جدولي. وبالمناسبة، إذا لم تكونوا هنا للغداء، فالرجاء ترك بطاقات الغداء، إن أمكنكم، للآخرين المتواجدين.

جولي هيدلوند: نعم. والآن استراحة القهوة لمدة 15 دقيقة. بعد ذلك لدينا ألين إينا حول تحول التسجيل في OpenDNSsec وبعدها داني جرانت حول DNSsec ككل، وبعدها الأسئلة.

دان يورك: حسنًا، مرحبًا. الجميع، سنذهب إلى الاستراحة بالفعل. لذا، لنأخذ استراحة، ولكن سريعة، رجاءً، حتى يمكننا العودة بأسرع ما يمكن ودعونا لا نبدأ بعد أكثر من 15 دقيقة. أليس هذا صحيحًا؟

جولي هيدلوند: أجل. حسنًا، سوف نبدأ بدونك.

دان يورك: سنبدأ ونريد أن نسمع ألين يتحدث عن ما يطرحه.

روس موندي: والساعة تسري على الاستراحة، أيضًا. إن كان أي منكم يرغب في العلم، فعليه فقط أن ينظر إلى الساعة.

دان يورك: خمس دقائق، رجاءً. يمكنكم تناول الشراب. أو مهما يكن. والعودة. نريد الاستمرار.

ثلاث دقائق.

روس موندي: دقيقتان في الاستراحة. رجاء البدء في العودة إلى مقاعدكم.

دان يورك: لذا، كما قال روس، دعونا نعود إلى مقاعدنا، إن أمكننا أن نبدأ بهذه الطريقة. وإن كنتم تجلسون في المؤخرة وتريدون الجلوس على الطاولة، فنحن نرحب بذلك أيضًا. هناك مكان فارغ. لذا، تفضلوا أيها السادة. دعونا نعود مرة أخرى. وتبقت لدينا دقيقة، ولكن تفضلوا. لنبدأ.

إذا كنتم ترون مساحة فارغة على الطاولة وتودون الانضمام لنا، فمرحبًا بكم. هناك واحد هنا، إن أراد أي منكم الجلوس بجواري، فمرحبًا بكم. أيًا كان. علينا العودة. جيد. وسنصل إلى ذلك. حسنًا.

هل نحن جاهزون؟ أوه، لا، كاثي، نحن لا نزال، نحن نقوم بالأمور. ماذا سنفعل؟ حسنًا. أجل، حسنًا. لذا، نحن جميعًا بخير. حسنًا. لا بأس. أود أن أقدم السيد الذي كان يتحدث ألان، والموجود هنا للحديث مرة أخرى. إذن سوف أحيل الكلمة إليه. وأنا أشرف على الأسئلة، لذا، إذا كانت لديكم أية أسئلة، فتفضلوا بالاستعداد لطرحها. نعم، ها هو.

آلين إينا: نعم. أنا آلين إينا من أفريقيا. وأريد فقط مشاركة الخبرات الخاصة بتحول DNSsec والتي حصلنا عليها في AFRINIC. لذا، نعم، أنا الآن [غير مسموع]، كنت في AFRINIC قبل ذلك، وقمت بهذا مع الفريق قبل أن أغادر. إذن [يتعذر تمييز الصوت]. نعم. حدث التحول في AFRINIC وربما على أن أوضح إدارة AFRINIC بصفتها سجل إنترنت إقليمي [غير مسموع] DNS للإصدارين الرابع والسادس [غير مسموع] AFRINIC.

تدير AFRINIC تسع مناطق ستة منها V4 وثلاث مناطق V6. كما أن AFRINIC تنفذ DNSsec منذ أبريل 2012، مقاضاة OpenDNSsec، ولسبب ما علينا التحول، وهذا هو سأعرضه. لذا، غن كنا سنذهب إلى الرابط الأول، فستعلمون عن DNSsec في AFRINIC والرابط الثاني يوضح بالضبط ما سأتحدث عنه.

لذا، السياق [غير مسموع] يتم استخدام OpenDNSsec من قبل DNSsec لتسجيل المناطق التسع. ويستخدم المفتاح في HSM [غير مسموع]. [غير مسموع] 56 وكذلك OpenDNSsec، التي نستخدمها في هذا الوقت كانت قاعدة بيانات SQLite. وطوال الطريق، واجهنا بعض المشكلات، مشكلات تسجيل المنطقة، بحيث تم تسجيله مرة إلى أخرى كعبارة فحسب. وبعد ذلك، فهي هذه الحالة، حدثت بعد التأخيرات في منشور المنطقة، وما قمنا به هو تنفيذ بعض العمل والذي تمثل في إعادة التشغيل، لإعادة تميل المعيار للجميع، وأعتقد كل ساعة، حسنًا، لدفع المحرك والعمل مرة أخرى. لذا، كانت هذه طريقة الحل حتى انتقلنا إلى هذا.

لذا، نعم، كما قلت، الدافع هو الانتقال إلى [غير مسموع] جديد، وهو ما يستند إلى OpenDNSsec، بتغيير قاعدة البيانات بحيث تسمح لنا بإضافة بعض المناطق. لقد أدرنا AFRINIC أيضًا DNS العامة والعديد من الأسماء للقارة، كما كانت تخطط أيضًا لبدء تسجيل الأعضاء. لذا، فقد قررنا أننا يجب أن ننتقل إلى قاعدة بيانات [غير مسموع] SQLite.

إصدار جديد من نظام البرنامج، وقد أردنا الحفاظ على المفتاح في نظام البرنامج، نفس الخوارزمية ونفس سياسة التسجيل. نعم التالية. لذا، لم تكن الإستراتيجية هي تصدير

مفتاح خاص أو بداية جديدة لأن المفتاح في نظام البرنامج. وكان عليكم الحفاظ على حالة التحقق لكافة المناطق كافة الأوقات، لذا، فهذا ما كان علينا القيام به أيضًا. وقد قررنا أننا لن نتعرض لهذا المفتاح الخاص.

كذلك، لا يمكننا البدء من جديد بسبب الخطة الثالثة. ونحن في طور الإصدار ولدينا أعضاء لديهم منطقة تسجيل، ومن ثم، علينا الحفاظ على حالة التحقق في كافة الأوقات. لذا، بعد ذلك، ما نقوم به، هو الترحيل مع استبدال المفتاح. هذا [غير مسموع]. فمن جانب، نرى [غير مسموع] القديم، والنظام يستند إلى الحصول على المنطقة من سجل رئيسي مخفي من خلال نقل المنطقة.

[غير مسموع] والدفع نحو السجل الرئيسي العام والذي ينقل بعد ذلك من خلال نقل المنطقة إلى خدمة الاسم الثانوي العامة [غير مسموع]. لذا، هذا ما قمنا به. ويمكنكم أن تروا هذا المنشور الكبير لمفتاح DNS و[غير مسموع]، لذا، لقد اخترتم المفتاح وتأخذون [غير مسموع]، وكذلك مفتاح الدخول الرئيسي من [غير مسموع]، ثم إلى [غير مسموع] القديم، قبل النشر. حسناً؟ ونضع أيضًا DS للمفتاح الجديد في IP [غير مسموع] كما نتعرض للمفتاح العام من [Sonya] القديم ثم إلى [Sonya] الجديد [غير مسموع] قبل نشر مفتاح DNS وتسجيل دخول [غير مسموع].

وبعد ذلك، في نقطة ما، حسب التوقيت، تتوقفون عن [Sonya] الجديد وننقل إلى [Sonya] الجديد. لذا، هذا قبل التحول. ويمكنكم أن تروا أن لدينا DS من الإشارة القديمة إلى DS للمفاتيح القديمة والتي استخدمت التسجيل سواء بالمفتاح القديم أو الجديد. حسناً؟ نعم التالية.

بعد التحول، فهذا ما نراه من جانبنا، في حين ترون المفتاحين، المعينين إلى مفتاح الدخول الرئيسي المستخدم للتسجيل سواء في مفتاح الدخول لمنطقة الجذر القديم أو الجديد، لذا، لديكم مفتاحان مع [غير مسموع] واحد. ولذا، عندما نقوم بهذا، كان النظام من مفتاح الدخول لمنطقة الجذر، لذا فبعض عمليات الاستبدال للمفتاح كانت [غير مسموع] والمفتاحين كما ترون هناك بنقطة [غير مسموع].

لذا، أعلنا عن التحول لبعض الوقت، وكان لدينا التسجيل بمفتاح الدخول الرئيسي القديم والجديد في العمليتين في اثنين من مفاتيح الدخول لمنطقة الجذر، ويمكن أن تروا هذا. بعد بعض الوقت، هذا [غير مسموع] ما ترون، قبل أن نستبعد المفتاح القديم، وبعدها المرحلة النهائية كانت استعاد DS منه للمفتاح القديم من مناطق IP [غير مسموع]. نعم التالية.

وبهذا، يتطلب هذا الموضوع إعادة نظر بحرص في التخطيط والتوقيت. وعليكم الحرص عند التسجيل بالتوقيع، وترك الوقت، TTM، للنظر في المفاتيح وحالتها، وما إليها، والإدارة بحرص عند التحول لأنكم تتذكرون أننا قلنا أننا نريد الحفاظ على حالة التحقق أو وقتها. لذا، ليس هناك مساحة للذهاب والتحقق والصلاحية لبعض الوقت. ومن ثم، نحتاج بالفعل للحرص. لذا، يعمل هذا بصورة جيدة، لا تعطل ولا تنبيهات. نعم التالية.

لذا، التجربة الجيدة وأعتقد أن هذا يمكنه أن يسري حتى إذا كنا سننتقل من تسجيل BIND إلى OpenDNSSEC أو BIND OpenDNSSEC، فأعتقد أن نفس الأمر يسري لأني أعتقد أنه يتعلق بإدارة المفتاح، حسنًا، أعتقد أن التجربة [غير مسموع] تسري أيضا على الانتقال من BIND لفتح الطريق الآخر. لذا، سيكون لدي قصة مختلفة للمفتاح في SSM في أمن الأجهزة، لذا، ربما لن نذهب إلى تصدير مفتاح خاص، على سبيل المثال، إذا كان لدينا مودم أمني للأجهزة، فربما يمكن أن يكون الخيار الوحيد هو إنشاء واحد جديد وجعله يتحدث إلى مفتاح [غير مسموع] في SSM.

لذا، المرة التالية، سأقوم بهذا، نفس الأمر باستثناء النشر المسبق لمفتاح الدخول الرئيسي. وقد قمنا بنشر مفتاح الدخول الرئيسي مع DS، والذي لم يكن لازمًا بالفعل لأننا يمكن أن نقوم بهذا فقط مع DS ولكننا قررنا أيضًا النشر المسبق لمفتاح الدخول الرئيسي لتجنب أي مشكلات، ولكن المرة التالية، أعتقد أن علينا القيام بهذا بدون النشر المسبق ونشر مفتاح الدخول لمنطقة الجذر مسبقًا وكذلك أن نقوم بهذا مع DS. أجل. شكرًا. وأرى أن هذه الشريحة الأخيرة. شكرًا.

دان يورك: حسنًا. لدينا وقت لبعض الأسئلة، وسأبدأ بهل يمكنك أن تتناول سبب أنكم لن تنشور مفتاح الدخول الرئيسي مسبقًا؟

آلين إينا: لا، حسنًا، لا يلزم هذا. حسناً؟ لأنه من خلال تنفيذ DS، فهذا يعني أن لديكم DS للمفتاح الجديد المنشور بالفعل في [غير مسموع] لذا ليست هناك حاجة للنشر المسبق. حسنًا. لأنه عندما يكون لدينا. حسنًا. الأمر مثل القيام باستبدال مفتاح الدخول الرئيسي. إن أردت استبدال مفتاح الدخول الرئيسي، فيمكنك القيام بالتسجيل، أو DS.

ولكن ما قمنا به هنا هو أننا قمنا بتغيير DS وتسجيل الدخول من خلال النشر المسبق للمفتاح [غير مسموع] مفتاح الدخول الرئيسي.

دان يورك: حسنًا. أحتاج للوحة بيضاء للتفكير في ذلك في عقلي أو شيء من هذا القبيل. ولدينا بعض الأسئلة بالفعل، وأرى أحدها من روبرت. وأذا كنت يا روبرت و[غير مسموع]، ارى في قائمة الانتظار. هل ثمة أحد آخر؟ حسنًا. دعوني أعلم إن لم تكونوا مهتمين. تفضل، روبرت.

روبرت مارتن ليجين: مرحبًا. روبرت من PCH. أتفق أنا وبن في أنكم لستم على صواب. ولكن، اللوحة البيضاء مرة أخرى، عن إعادة النشر. حسنًا، الأمر هو أنه عندما تنشرون مفتاح الدخول الرئيسي مسبقًا، فلديكم توقيع معين على سجل الموارد الرئيسية في DNS، وقد يتم تخزين هذا في مكان ما. وهذا هو الموضع الذي قد تتعرضون فيه للمشاكل بالفعل.

مع ذلك، ان لم يختر أي شخص هذا، فهذا لا بأس به. وسؤالي كان خلال هذا التمرين عن طرح المفاتيح، هل تتشاورون مع أي RFC خارجي لأفضل ممارسات DNSsec أو شيء ما يتعلق بكيفية تنفيذ المؤقت وما إلى ذلك؟ هناك طلب تقديم تعليقات حول كيفية تنفيذ DNSsec. ولديهم أيضًا بعض الأقسام حول التنفيذ الفعلي للعمليات. فهل تتشاورون بشأن طول مدة الانتظار قبل كل خطوة وأمور من هذا القبيل؟

آلين إينا: نعم، بالتأكيد، كما قلت. فإدارة الوقت في DNSsec مهمة للغاية. لذا، نعم، عندما ننظر في RFC وأيضًا بعض الوثائق [غير مسموع] شخص ما قام بالفعل بشيء مماثل ونشر بعض الموارد، ولكننا، نعم، كما قلت. يرجع ذلك إلى أننا نحتاج للحفاظ على سلسلة الثقة [غير مسموع] وبعدها كان علينا النظر بالفعل في السياسات الخاصة بنا، وسياسة تسجيل الدخول والوقت والتصميم حتى يتوافق النظام مع الحاجة بالضبط. ولكن نعم، لقد قمنا باستخدام أفضل الممارسات من RFC. أجل.

[بن]: بن [غير مسموع]، مختبرات. حسنًا، أحد جهات صيانة OpenDNSSEC. لذا، شكرًا جزيلاً لكم على هذا العرض ومشاركة الخبرات. ونتطلع دائمًا لمعرفة الجيد والسيء والقبيح. وهذا نوع من التعقيبات مفيد للغاية، كما أنه ما يمكن تحسينه، بالطبع.

كذلك، فيما يتعلق بالتوقيت، لذا، [غير مسموع]، عندي فضول للمعرفة. وأعتقد أن يفضل أن يكون واحد لواحد. فما هو [غير مسموع]؟ وما هي سياساتكم؟ يعتبر OpenDNSSEC 2.0 قريبًا أو إصدارًا عامًا، وهناك طريقة مرنة أكثر لتحديد السياسات وتفعيلها في استبدال المفاتيح.

آلين إينا: لذا، نعم، رأيت هناك على [غير مسموع] شرحة ثانية، وقد نشرنا بعض المعلومات حلو هذا في مدونة AFRINIC، [غير مسموع] لدينا، إذا كنتم بالنسبة للرابط الأول الموجه إلى [غير مسموع] ، لدينا على الرابط الأول الذي يوجه إلى DNSsec في AFRINIC حيث يمكنكم أن تروا DPS، وموقع الخط الثاني يأخذكم إلى الموضوع. ولكن، يمكننا عند الحاجة لمزيد من المعلومات، يمكنني، حسنًا.

دان يورك: جيون، رأيتك.

جيوف هوستن: أجل. أعتقد أنكم ستعثرون على هذا RFC 6781 وهي الوثيقة التي تبحثون عنها. وبالفعل إذا نظرتم في 6781، فهي تحلل مجموعة الطرق بالكامل التي يمكنكم من خلالها استبدال المفتاح. وبالأساس، إذا كنتم ستقومون بالتسجيل المزدوج وفترة يكون فيها كلا المفتاحين نشطًا، فبذلك تمت زيادة حجم المنطقة وحجم الردود. وربما يترتب على هذا زيادة حجم استجابة DNS وهو ما قد يكون مشكلة.

لذا، يمكنكم القيام بهذا على مراحل لا تتضمن التسجيل المزدوج، ولكن هناك حلول وسط أيضًا. والأمر غير مناسب لضعاف القلوب. حيث تمت كتابة 6781 للزملاء الذين يفهمون DNSsec. لكن، إذا كنتم ستشرعون في طرح المفاتيح، فربما تحتاجون لفهم DNSsec. لذا، فالوثيقة لا بدء من قراءتها بالفعل. وليس عليكم طرح المفاتيح حتى تفهموا RFC، ثم سيكون لا بأس بذلك. شكرًا.

آلين إينا: شكرًا لك جيوف.

دان يورك: هل ثمة أسئلة أخرى موجّهة لنا؟

روس موندي: شكرًا لك، دان. شكرًا لك، ألان. عرض مفيد جدًا. سؤالان. الأول، سابقًا في اللجنة الإقليمية الأفريقية، كان هناك قدر معقول من النقاش حول بطء التعامل مع التحقق من المناطق المسجلة والاستخدام الفعلي لها. وقد كان لدي فضول إن كنتم قد حددتم طريقة قياس أو بصورة ما تجميع البيانات فيما يتعلق بما يقترب على الأقل من المستخدمين النهائيين؟ وكذلك، كيف تحققتم مما إذا كان هناك تعطل أو بطء أو مشكلات في أحجام الردود. بالنسبة للمناطق الرئيسية، هل هذه المناطق مستخدمة، وهل يمكنكم الحديث قليلاً عما قمتم به في هذه المنطقة؟

آلين إينا: هل تتحدث عن الوضع خلال طرح المفاتيح، أم بصورة عامة؟ لا.

روس موندي: خلال طرح المفاتيح بصورة خاصة، إذا كانت هناك قياسات نظرتم فيها أو مختلف الأماكن التي عملتم معها لتجميع البيانات.

آلين إينا: نعم، حسنًا. خلال طرح المفاتيح، حسنًا، استخدمنا DNS [غير مسموع] معظم الوقت، ولكن أيضًا محلل ما من، مثلاً، لم أقم بهذا عن بعد. لذا، فقد كنت في توجو، وكنت أتابع هذا باستخدام المحلل في توجو، ثم كان التشغيل في جنوب أفريقيا. بعد ذلك، كانت لدينا أيضًا رؤية من موريشيوس بالإضافة لما حصلنا عليه من DNS. لذا، فهذا كيف تابعنا طرح المفاتيح للتأكد من عدم تعطل أي شيء. أجل. لا تعطل.

روس موندي: رائع، شكرًا. وستسمعون هذا مرة أخرى ربما من دان ولاحقًا مني. القياس وتجميع البيانات لأن هذا مهم للغاية. كذلك، ليس لدينا هذا القدر من البيانات ونريد بالفعل تجميع المزيد.

آلين إينا: حسنًا، لا، بالتأكيد.

دان يورك: وأود أن أكرر أيضا، أني سأقول ما قالته جولي وأطلب من الناس قول أسمائهم وانتماءهم عند الحديث عبر الميكروفون للزملاء الموجودين. وبهذا، سأسلم الميكروفون إلى الشخص بجواري. تفضل.

وفاء داهماني داعفوري: وفاء من تونس. أردت فقط أن أعلق على ألين. كما تعرف، ألين، شكرًا لكم على دعم ودعم AFRINIC اليوم [غير مسموع] لتعيينه، وهذا نوع من [غير مسموع]. مع ذلك، علينا أن نقوم بعمل آخر أيضًا، الخطوات اللاحقة. وعلينا الآن تسجيل كافة المناطق، كما أن لدينا الكثير من العمل مع أمناء السجل. وأردت إضافة شيء. أنت أحد أفضل مدربي DNSsec على الإطلاق.

آلين إينا: هل يمكنني التعليق على ذلك؟

دان يورك: بالتأكيد.

آلين إينا: لا، [غير مسموع] لقد عملت في ATI وATI [غير مسموع]. إن كنت ستنظر في الإحصائيات من المنطقة المقابلة في AFRINIC فإن ATI و[غير مسموع] أضافت شخصين سجلاً ثم دفعا DS إلى التحول إلى [غير مسموع] وقد ساعداني بالفعل في لمعرفة ما هي AFRINIC بأني كنت أقوم بشيء ما.

دان يورك: هل يود أي شخص آخر أن يتدخل؟ ورائي؟ هل من أحد؟ حسنًا. حسنًا. أردت أن أشكر ألين على طرح هذا المثال. وهي أحد الأمور التي نسأل فيها عادة. وسأضع ملحوظة هنا، للجلسة التالية في ICANN 56، وهي أننا نبحث عن هذا النوع من دراسات الحالة أو الأمور التي يتحدث عنها الناس عما يقومون به، وما يمكن أن يقوموا به بصورة مختلفة؟ ماذا سيفعلون في هذه الحالة؟ وكيف سيقومون بهذا العمل؟

لذا، رجاءً، إذا كنتم تقومون بهذا، وستودون في القدوم والعرض والتحدث، فيمكنكم معرفة أننا لا نطرح أسئلة صعبة للغاية. فنحن لا نأكل الناس أحياء. ربما يفعل هذا البعض، ولكننا نقدر ذلك بالفعل. شكرًا ألين.

لاحقًا، لدينا متحدث جديد بيننا، سيسعدنا أن نستمع إليه. والعديد منا على علم بأن CloudFlare قدمت موجات كبيرة عبر السنة الماضية من خلال الإعلان عن أنهم سيتيحون التسجيل لملايين النطاقات لديهم التي كانت موجودة. وأولافور، المتواجد دائمًا، ولكن في بعض الأحيان، لكنه عادة هنا.

فقد أتي وتحدث إلينا قبل ذلك عما سيقومون به والخطوات التي سيتم وأولافور وجاك، من يجلس هناك، أو كان هناك. أين جاك؟ لقد غادر أيضًا. حسنًا، لقد غادر الناس. وقد كانوا يعملون على كيفية أتمتة بعض هذا إلا أن داني جرانت هنا سيتحدث لنا عما تقوم به CloudFlare، وكيفية تنفيذ تسجيل DNSsec واسع النطاق لملايين النطاقات. ها هو ذا.

داني جرانت: مرحبا بكم جميعا. أنا داني، مدير المنتجات في DNS. وهذا مشابه للغاية للغرور الذي عليكم تقليله. حسنًا. أنا مدير المنتجات في CloudFlare DNSsec. وCloudFlare تتولى مسؤولية حوالي 4 مليون نطاق. على أننا نجيب كل يوم على 43 مليار استعلام DNS عبر 76 موقعًا. ومنذ حوالي أربعة شهور، أطلقنا DNSsec لأي نطاق مجانًا.

على نطاق مستوانا، كان هذا تحديًا. وكان علينا أن نتحلى بالإبداع الشديد في عملية التنفيذ، ونريد أن نشارك معكم الخطوات التي نتخذها لتنفيذ DNSsec العالمي. الشريحة التالية. بالتحديد، كيف يمكننا اختيار خوارزمية التوقيع، وكيف نحافظ على حساب الدوائر حول الإجابات السلبية وما نتعلمه حول دعم أمناء السجل والسجل للبروتوكول. الشريحة التالية والتالية لها.

يتمثل الاختصاص الرئيسي في CloudFlare في تلافي DDOS. وعادة ما تتلافى CloudFlare هجمات كبيرة بدرجة 400 مليون مجموعة كل ثانية. في هذا الصدد، كانت الهجمة على L-root في نوفمبر فقط 5 مليون مجموعة كل ثانية، وبالتالي 80/1 من الحجم.

تتمثل أحد الطرق التي تستخدمها مواقع الحرمان المنتشر للخدمة المهاجمة في القيام باستعلامات متكررة على DNS يكون لها أحجام استعلام صغيرة ولكن إجابات كبيرة. وبعد ذلك، يستخدم المهاجمين عناوين IP مخادعة بحيث ترسل هذه الإجابات الكبيرة إلى الخادم الذي يهاجمونه. ارجع للوراء للشريحة السابقة.

تعتبر المناطق التي بها DNSsec، بسب بعض أحجام هذه الإجابات، فرصة مناسبة عادةً لهذا النوع من إساءة الاستخدام. وفقط في الشهر السابق، نشر أكاماي تقريرًا أمنيًا حول كيف يتم استخدام بعض نطاقات gov. لهذا النوع من الهجمات الموسعة. في هذا الصدد، تخيل إذا كان يمكن استخدام كل نطاق في DNSsec على CloudFlare لهذا النوع من الهجمات الموسعة، فنحن بالضرورة نجعل نفسنا هدفًا.

لذا، لهذا السبب، اتخذنا التدابير، الشريحة التالية، للتأكد من أن كل إجابة من DNS نرسلها تتوافق مع مجموعة يكون حجمها أقل من 512 بايت، حتى مع DNSsec. وأحد الطرق الرئيسية التي نقوم بهذا من خلالها هي تكون باستخدام خوارزمية التوقيع الرقمي ذو المنحنى الإهليجي، ECDSA، وهي خوارزمية DNSsec رقم 13، والتي تتركنا نستخدم المفاتيح الصغيرة والتوقيعات الأصغر. الشريحة التالية.

هذا عالم رياضيات ألماني، أجرين لينسترا، والمشهور بحديثه عن التشفير من حيث الطاقة. على أنه يأخذ قدر الطاقة المطلوبة لكسر أجزاء الشفرة ويقارن ذلك بمقدار المياه التي يمكن أن تغليها الطاقة. الشريحة التالية.

لذا، فلكسر RSA 228 بت، يأخذ هذا مقدار من الطاقة لغلي ملعقة مياه. قارن هذا، الشريحة التالية، مع مفتاح ECDSA بنفس الحجم. ولكشر هذا، سيأخذ طاقة كافية لغي كافة المياه على وجه الأرض. لذا، يتيح استخدام ECDSA لنا استخدام مفاتيح أصغر بأمن مماثل. لذا، نستخدم مفتاح ECDSA 256 بت، وهو ما يعادل في القوة مفتاح RSA 3100 بت. وتكون معظم مفاتيح RSA 1024 أو 2048 بت. الشريحة التالية.

لذا، يمكنكم أن تروا ماذا يفعل ذلك لحجم المجموعة. الشريحة التالية. وهذه ميزة أخرى في ECDSA وهي أنها سريعة. حيث يمكن أن تنشئ CloudFlare الآن 57 مليار توقيعًا يوميًا، مع الاهتمام كثيرًا بتكلفة الحوسبة. الشريحة التالية.

لذا، فكرنا أن ECDSA كانت سريعة ومن ثم، فأحد المهندسين لدينا، فلاس كراسنوف، نفذها وحصل على سرعة تصل إلى 21 ضعفًا. وهذا بالفعل الآن جزء من تشفير Go 1.6، ويأخذ الآن من CloudFlare جزء من الثانية، حرفيًا 0.0001 من الثانية لتسجيل سجل DNS. الشريحة التالية من فضلك.

حسنًا، إجابات بالنفي. الشريحة التالية. توجد مشكلتان في الإجابات النفي. الأولى أنها تتطلب من الخادم المعتمد إعادة الاسم السابق والتالي. أما في CloudFlare، فهي مكلفة من الناحية الحسابية، ويمكن أن تؤدي إلى تسرب المعلومات حول منطقة. والمشكلة التالية هي أن ذلك يتطلب اثنين من سجلات [NSEC] واثنين من التوقيعات اللاحقة لمصادقة عدم وجود أحد الأسماء غير الموجودة.

لذا، سأتحدث أولاً عن الاسم السابق والتالي. وهناك بضعة بيانات أساسية حول DNS. تستخدم CloudFlare خادم DNS مخصص مكتوب فيما يسمى RRDNS والتي ترمز بالفعل إلى Ray Ray DNS على اسم راي بيجاني، الذي كان مهندسًا للأنظمة في CloudFlare وأحد المهندسين الأساسيين في المشروع.

وسأكون موجزًا للغاية بوضوح. الأمر الفريد في RRDNS هو أنه ليس هناك مفهوم لملف المنطقة. بدلاً من ذلك.

دان يورك: داني، هل يساعدك هذا. لدي المشكلة ذاتها. حسناً؟ وعندما بدأت الانطلاق هنا، أخبرني الناس "دان، لا ترد كثيرًا." لا عليك. فلدي صحبة رائعة.

داني جرانت: لقد وجه إلي تحدٍ حتى بأن أكون أسرع. حسنًا. حسنًا، حسنًا. لذا، RRDNS. الأمر الفريد في DNS لدينا هو أنه ليس هناك مفهوم لملف المنطقة. وبدلاً من ذلك، لدينا قاعدة بيانات SQL مستوية، وتحمل كافة سجلات DNS لكل منطقة في CloudFlare. وعندما تلقينا استعلام DNS للسجل، فقد انتقلنا فحسب إلى قاعدة البيانات واخترنا السجل الذي نحتاجه.

أما الجانب الآخر الفريد في RRDNS فهو أن هناك الكثير من المنطق التجاري في DNS. وعادة ما تقوم CloudFlare بإنشاء إجابات سريعة، لذا، لا نعرف دائمًا كيف سنرد قبل أن نقوم بهذا، الشريحة التالية.

مشكلة أخرى، حسنًا. عادة مع الإجابات بالنفي، يلزم أن يقوم الخادم المعتمد بإعادة الاسم السابق والتالي. أما في CloudFlare، فبدون الرؤية الكاملة لملف المنطقة، سيكون علينا أن نطلب أن تنفذ البيانات بحثًا مصنفًا فقط للعثور على الاسمين السابق والتالي. ومع الإجابات المتغيرة، سيكون من الصعب علينا أهن نعرف حتى ما هي الأسماء السابقة والتالية بدون الاحتساب المسبق لكافة المخرجات المحتملة.

أما المشكلة الثانية، فتتمثل في أن الاسم السابق والتالي يمكن أن تعرض معلومات المنطقة. فهي تعرض الأسماء الموجود في منطقة للكشف. والحل الشائع لهذا هو NSEC3، ولكن حتى هذا يمكن اختراقه بهجمة قاموس. الشريحة التالية.

هذا هو الحل المقترح للأسماء السابقة والتالية، وهي RFC 4470، بعد التعديل من وايت لايز. وتقول وايت لايز "حسنًا، يمكن أن يقوم مشغلو DNS بالإنشاء العشوائي للأسماء السابقة والتالية من خلال العثور على شيء قانوني إلى حد ما قبل وبعد الاسم المفقود." هذا رائع. وهذا يساعد في منع كشف المنطقة والمزيد من عمليات البحث في قاعدة البيانات. لكي لا يزال هناك اثنين من سجلات NSEC المسجلة بصورة مستقلة يظهران كشيء واحد. الشريحة التالية.

في CloudFlare، قررنا اتخاذ الكذب كنهج إلى أقصى درجة. وبدلاً من وايت لايز، تمثل CloudFlare بلاك لايز. هذا مثال على ما نقوم به عند عدم وجود بيانات. وعندما يوجد الاسم ولكن ليس من النوع المطلوب، فنحن نقول "حسنًا، كل نوع موجود، ولكن فقط ليس النوع الذي طلبتم." لذا، فعند طلب TXT، نقول "نعم، حسنًا، لديكم حظ سيء. ولدينا كل نوع، وليس TXT فحسب." كذلك، عند طلب MX، فسنقول "لقد فاتتكم مرة أخرى. ولدينا كل نوع، بما في ذلك TXT ولكن ليس MXفحسب." الشريحة التالية.

هذه هو ما يقوم به هذا في حجم المجموعة. لذا، فالإجابات بالنفي حوالي 300 بايت. وعلى سبيل المقارنة، بالنسبة للإجابات بالنفي في IETF.org وICANN.org، فإن

الأولى تستخدم NSEC بينما تستخدم الثانية NSEC3، وهو يزيد قليلاً عن 1000 بايت، لذا، فنحن ثلث حجم المجموعة، وهو ما يبدو مناسبًا بالفعل. كذلك، يوفر لنا هذا عمليات البحث على قاعدة البيانات وخاصة حيث أن العديد من الهجمات تقدم فحسب إجابات بالنفي عشوائية، وهذا تدبير فعال للغاية بالنسبة لنا. الشريحة التالية.

حسنًا. بخلاف التحديات التقنية في DNSsec، تتمثل أحد الاعتبارات في نشر DNSsec واسع النطاق في تكلفة الدعم للحاجة للتوضيح للمشتركين فيما يتعلق بسبب أنهم لا يدخلون ويضيفون DS لدى أمين السجل إذا لم تتم إضافة أمين السجل أو السجل لدعم DNSsec أو الخوارزمية 13 والتي تمثل خيار خوارزمية التوقيع. الشريحة التالية. التالي.

أريد أن أوضح لكم بعض الأمور التي يقوم أمناء السجل -- سنًا. لذا، عادةً، هذا نوع الإثارة هنا. عادة، عندما يذهب المستخدمون إلى أمناء السجل، فهم يلتقون مع فرق الدعم التي لم تسمع يومًا عن DNSsec أو تقدم لهم معلومات غير دقيقة. لذا، ما أريد عرضه عليكم هو بعض هذه المعلومات غير الصحيحة التي يتلقاها المستخدمون من أمناء السجل.

لذا، فهذه واحدة من أمين سجل كبير للغاية. وهناك بعض اللبس هنا حول من يمكنه إضافة DS. يقول أمين السجل للمستخدم "حتى تتيح DNSsec، يجب أن يكون اسم النطاق تحت إدارة DNS لأمين السجل، وهو ما يعني أن النطاق سيحتاج للانتقال إلى خادمنا. ولم تكتمل التغييرات وتم إغلاق الطلب." وهذا الأمر غير صحيح. حيث يمكنهم إضافة DS حتى إذا كان المستخدم يستخدم خوادم أسماء لجهة خارجية. الشريحة التالية.

هذه واحدة أخرى. أخبرنا مستخدم (تحدثت إلى فريق الدعم لدى أمين السجل وقد قالوا أنني يجب أن أدخل سجل DS لديكم حيث أن DNS الخاص بي مستضاف هنا." مرة أخرى، هذا الأمر غير صحيح. التالية هي المفضلة لدي.

هذه دردشة مع أحد أمناء السجل. ويقول فريق الدعم لدى أمين اسجل "لم يعمل بعد خيار DNSsec. ومن ثم، لا نقدم الدعم له بعد." ويوضح المشترك، "لذا، إن أضفت سجل DS الذي ينص على "DNSsec نسط،" أليس معنى هذا أن DNSsec نشط بالفعل؟" والدعم يقول "بالضبط."

لدينا عملاء أرسلت إليهم ملفات PDF للملء حتى يضيفوا سجل DS. وقد تلقى أحد العملاء حتى نص بيرل لتشغيله، وقد كان رائعًا. ولكنه هذا هو الوضع في العالم حاليًا. الشريحة التالية.

توجد أيضًا حالات جيدة للغاية. أضاف كثير من السجلات وأمناء السجل الدعم في DNSsec للخوارزمية 13 منذ إطلاقنا إياها. الشريحة التالية.

تقوم no. حتى بتشجيع دعم DNSsec لأمناء السجل من خلال توفير خصم على النطاقات المسجلة. لذا، فهذه مشكلة كفاءة كبيرة وهذا الدليل هو نسخة من DS في منفذ أمين سجل وهو شيء يمكن أتمته بل ويجب ذلك. كذلك، سنود في CloudFlare أن نتمكن من إرسال سجلات DS تلقائيًا إلى أمين السجل أو السجل، ولكن قواعد ICANN صارمة بالفعل فيما يتعلق بالمؤسسات التي يمكن الحديث إليها من المؤسسات الأخرى وأسماء النطاقات. لذا، يمكن أن يتحدث أحد أمناء السجل إلى سجل ولكن مشغل DNS مثل CloudFlare لا يمكنه ذلك. انتقل شريحتين.

على طول الجانب الأيمن، سارة، وRed Hat، لقد نشرنا مسودة على الإنترنت تقترح طريقة لأتمتة DS، أتمتة إرسال DS إلى أمناء السجل والسجلات. ولا توجد سوى بضعة سجلات وأمناء سجل، وهو ما يعني أنه بالسنة المقبلة، سنتمكن من إتاحة DNSsec تلقائيًا لبضعة مئات الآلاف من النطاقات. الشريحة التالية.

هل هناك أي أسئلة؟

دان يورك: أشك أن الأمر سيكون كذلك. ليس أقل من هذا، ربما من المترجمين يحاولون الفهم. ولكن لا، أرى قائمة انتظار هنا، وجولي تخبرني، ماذا لدينا عن بعد؟ حسنًا، كما أرى [ديمتري] أولاً لأنه يجلس بجانب داني، تفضل ديمتري.

ديمتري: حسنًا، لا بد أني محظوظ. وقبل أي شيء لدي تعليق. في UAV، نفذنا 13 بالفعل، وكان لدينا اختبار [غير مسموع] في CloudFlare، تم إطلاق الخاصية بفضل مارتن ليفي، الذي دعم هذا. وهو URL اختباري، يمكننا حتى اختباره. إن كنتم تريدون شرطتين MQA [غير مسموع].

مع ذلك، يتمثل التعليق الثاني في الترتيب في أمر واحد، وهو مرة أخرى، استخدام الميزة، ويمكنني أن أعرضه لكم على الشاشة. يمكنكم النظر إليه هنا. هذه واجهة [غير مسموع]. حسنًا، حيث لا يمكنكم رؤية هذا، ولكني يمكنني أن أقدم لكم نسخة [غير مسموع] إلى أي شخص يريد هذا. والتوضيح التفصيلي للسجل من النوع S في قاعدة بيانات إدارة [غير مسموع] ليس به النوع 13. فلديه ثلاثة وخمسة وستة وسبعة وثمانية وعشرة. لذا، إذا عرفت يد ذلك، فلن تعرف الأخرى، والحديث بالفعل إلى السيد كيم ديفيز منذ عامين على ما أعتقد.

على أي حال، لا يزال التنفيذ معلقًا. وربما سيتضمن العقد الجديد هذه الخاصية.

دان يورك: الاستعداد للحديث في 1:15 حيث نتحدث عن كل [غير مسموع].

[ديمتري]: أجل. أنا متأكد أنها ستحل على الفور. وهذا ما أردت توضيحه إلى حد كبير. وشكرًا على العمل الرائع.

دان يورك: حسنًا. عن بعد. هل تريد الانتقال إلى المشاركين عن بعد؟

جولي هيدلوند: أجل. أنا جولي هيدلوند من العاملين في ICANN، وأقرأ سؤالاً عن بعد، وسأذكر الجميع هنا فحسب. الرجاء عدم ذكر الاسم والانتماء عند الحديث. هذا سؤال من ماركوس من Global Village. وهو يقول "أفهم أن خوارزميات التوقيع الرقمي ذو المنحنى الإهليجي عرضة لهجمات الحوسبة الكمية، إذا أصبحت أجهزة الكمبيوتر الكمية واقعًا، بينما ليس الأمر كذلك في خوارزميات RSA. هل تعتبر هذا مشكلة؟"

داني جرانت: إذا أصبحت أجهزة الكمبيوتر الكمية واقعًا.

دان يورك: إن كان لدينا جهاز لنختبره. أعني، نحن نستمر في الجلسة عصر اليوم مع الحديث عن تشفير المنحنى الإهليجي على وجه التحديد، لذا، أشجع السيد على التعليق والإصغاء لذلك لأننا سنتحدث عن ذلك، ويمكنه طرح السؤال بالتأكيد حينها. أولافور، هل تريد الإجابة؟

أولافار جوموندسون: RSA دائمًا ما تكون عرضة.

دان يورك: نعم، حسنًا. أرى لارس هنا ورأيت مارك هناك وروبرت أيضًا. حسنًا. لذا، لارس. ولكنك لن تذهب بعيدًا. لذا، لننتقل إلى روبرت. حسنًا. تفضل.

لارس–جون ليمان: يمكنني استخدام هذا. لارس ليمان من Netnod. ولدي قليل من الفضول بشأن بلا لايز، ويجب ربما أن أتحدث إلى أولافور بدون اتصال. ولكن إذا كنت ستكذب بالبقاء خارج نوع السجل المحدد المطلوب، فهل هناك أي مخاطر من وصول العميل لهذه المعلومات؟

داني جرانت: تتضمن الإجابات بالنفي أقل قيمة TTL محتملة لهذا السبب. وهذه أيضًا الطريقة التي نبرر بها أن المنطقة يمكن أن تتغير خلال الفترة الزمنية التي يتم سؤالكم فيها.

دان يورك: غير مترابط. حسنًا. مارك.

مارك إلكينز: أجل. أحب هذا الكذب الأسود. والوضع عندما تضعون سجل DS في المنطقة ويقول "تم تسجيلDNSsec، نعم،" ولكنه ليس كذلك. فهذا بالفعل ما نقوم به في [غير مسموع] وهذا ببساطة لأنكم يمكنكم وضع مفتاح DS في السجلات ونعم، لم يتم تسجيله. وهذه هي حقيقة ما يحدث.

داني جرانت: هذا مثير. أعتقد أن الوضع الأفضل هو إضافة DS، حيث يتم نشره إلى الأصل، وتسجيل كل شيء. أفضل وضع.

دان يورك: حسنًا. لدي روبرت.

روبرت مارتن ليجين: أجل. روبرت من PCH. أحب أنكم تستخدم المنحنى الإهليجي لأنه لا يبدو لي أن أحدًا غيرك سيقوم بالكثير من هذا. فهل لديك أي فكرة عن المقدار، إذا كان شخص ما لديه مشكلة بالفعل مع التحقق من هذا؟ هل يمكنكم قياس هذا؟

دان يورك: الاستعداد للحديث في 1:15 من جيوف هيوستون.

داني جرانت: سوف أقدم ردًا سريعًا على ذلك. عندما بدانا تطوير خوارزمة 13 في DNSsec، كان هناك محلل واحد لم يكن لديه دعم، ولكن منذ ذلك الحين، أضافت DNS العامة من جوجل الدعم.

روبرت مارتن ليجين: حسنًا. تعليق أخير. لدي تعليق حول الكذب الأسود. وربما يجب أن نسميه الكذب المخيف لأنه يخيفنا قليلاً، كما أعتقد.

داني جرانت: لدينا صندوق اقتراحات في المكتب.

دان يورك: حسنًا. لدينا سؤال عن بعد.

جولي هيدلوند: شكرًا لك، دان. هناك سؤال عن بعد من أنطوني [غير مسموع]. إنه [غير مسموع]، يدرجه كتعليق ولكنه بالفعل ينتهي بسؤال. وهو يقول، "لا يعتبر عدم تمكن مشغلو DNS من الحديث إلى السجلات مشكلة تقنية ولكنه خطأ في نموذج ICANN. فماذا يحدث لإقناع مجتمع ICANN بتغيير النموذج لزيادة الأمن والاستقرار؟"

داني جرانت: حسنًا. بالنسبة للتعليق، نعم، أتفق. والإجابة على هذا السؤال، ماذا يجري القيام به؟ إثبات المفهوم. لذا، الآن، نحن نعمل مع بضعة سجلات وبضعة أمناء سجل على اعتماد مسودة الإنترنت، وبعدها أعتقد أن الطريقة الوحيدة للتقدم هي توضيح أنها تعمل بأمان.

دان يورك: سؤال آخر. أولافور؟

أولافور جوموندسون: أنا أولافور جوموندسون من CloudFlare. ونحن نقوم بهذا التجارب وإثبات المفاهيم في نطاقات ccTLD ويسعدنا العمل معها لإظهار نجاح هذا وعمله بصورة جيدة، لذا، يمكنكم التحدث غلينا بعد ذلك أو إرسال بريد إلكتروني لاحقًا.

دان يورك: حسنًا، حان دوركم.

شخص غير محدد: [غير مسموع] .dk. [غير مسموع] في دبلن على حديثكم هناك، ومن حينها، غيرنا [غير مسموع] بحيث تتيح لنا الحديث مباشرة. أنا أعمل الآن على الخوارزمية 13. استعداد.

دان يورك: أرى جيوف هناك.

جولي هيدلوند: لدينا ميكروفون متنقل لمن ليست لديهم ميكروفونات. وربما ليست فكرة جيدةأن [غير مسموع]، كما تعرفون.

دان يورك: جيوف، معذرة. لا؟

جيوف هوستن: لا.

دان يورك: حسنًا. هل يود أي شخص آخر أن يتدخل؟ لذا، أود أن أشكرك داني. وهذا مذهل، وقد أصبحنا معجبين، كما أعتقد بجهود CloudFlare في دفع هذا لبضعة مستويات. كما أن أحدها يحصل على المزيد من CDN واسعة النطاق بجانب مزودي خدمات

الاستضافة للقيام بهذا، وأيضًا للدفع على المنحنى الإهليجي. كانت هذا خطوة ضخمة للأمام في هذا الصدد. لذا، شكرًا لكم على جميع هذا وعلى العرض.

لذا، بصورة ما، يبدو أننا انتهينا من شيء هنا، وهو مثير. ربما كذلك، لأنه، ربما كانت سرعة داني. قد يكون الأمر هكذا. ونحن نتقدم بالفعل عن الوقت بعشر دقائق، وهذا لا بأس به لأن لدينا الكثير لنتحدث عنه، حسنًا، جولي تقول شيء ما.

جولي هيدلوند: حسنا، مع مراعاة أن الغداء محدد له الظهر، يتوقع منا أن نتواجد هناك في وقت الظهيرة. ولكن سألاحظ أيضًا. كما لاحظ بعضكم، كان هناك غداء معد في القاعة ولم يقصد ذلك. فمن المفترض أن تكون قاعة مختلفة. وهي جميعًا مجرد أسماء مختلفة هنا. لذا أخذنا ذلك بعين الاعتبار. ونحن متأكدين للغاية [غير مسموع]، وهو أكثر من مريح ومكان رائع لتتناول الغداء.

دان يورك: حسنًا. لذا، سأقوم وأتحدث. حسنًا. متنقل، نعم، حسنًا، جيد. فحص، واحد، اثنان. عليكم جميعًا تجربة هذا الشيء الرائع. توجد أوراق حولنا. ماذا في هذه الورقة؟ نعم. ربما نحتاج لقلم. وهناك هذه المفاهيم القديمة. أعتقد أننا في العصر الإلكتروني، ولكن شخص ما قدم لي هذه. فما مدى طول الوقت المستغرق، بالمناسبة، لاكتشاف أن القلم الذي كان في حقيبتي، كان مصباحًا أيضًا؟ أيضًا. حسنًا. حسنًا، تعني أنه قلم، نعم. هنا، نحن محظوظون، أمكنك القيام بهذا. أوه، إنه قلم.

أوه، حسنًا. حسنًا. لذا، هذه هي الصفقة. لدينا قليل من المتعة هنا، وبالنسبة للجدد هنا، فهذا هو اختبار DNSsec. وهو رائع بالفعل، حيث نسميه اختبار DNSsec الرائع، لكن بعض هذا بخصوص DNS أيضًا. لذا، لديكم جميعًا ورقة، وما ستقومون به.

والسبب في أن لدينا شريحة اسم هنا هو منع الغش. ونحن نكمل هذا ثم نقدمه إلى شخص بجوارك لتصحيحه. حسناً؟ حسنًا. نريد أن ننتهي من هذا حتى نذهب إلى الغداء لذا، واحد. حسنًا.

ليس هذه الأسئلة لي. حسنًا. روي أريندس، من Nominet. لا، روي آريندس من ICANN. عذرًا، كان روي موظفًا في Nominet لفترة طويلة يتعامل مع هذه الأمور ويقوم بتلك، لذا، فقد انتقل مؤخرًا إلى ICANN، حيث حضر منذ بضعة اجتماعات أو ما شابه، ولكن على أي حال.

كما قام باول ووترز ببعض هذه وكذلك وارن والأشخاص الآخرون. لذا، هنا نمضي ما مع قام به روي. لذا، ستقدم إجابة أو سؤال مطروح هنا. وسأنبهك من أنه في بعض الحالات، توجد إجابات متعددة. حسناً؟ إجابات صحيحة متعددة. ونعم، عندما نعود إلى هذا يمكننا النزاع عليها، ولكن في حالة النزاع، فأنا محق.

حسنًا، هيا لنبدأ. استخدم الظهر. لا، استخدم النموذج. ويمكنك تشكيل مجموعة أو اللعب لوحدك. ضع اسمك على النموذج. حسنًا، سنقوم بهذا. حسنًا. ها نحن ذا. في بعض الأحيان، توجد إجابات أكثر صحيحة. والنقاط تسجل لكل إجابة صحيحة، لا توجد نقاط، إذا كانت هناك إجابة خاطئة.

أي من نطاقات المستوى الأعلى هذه لا تنشر DNSsec؟ هل هي أ) EC؟ ب) MA؟ ج) TV؟ د) MX؟ ويمكنك كتابة هذا على الورقة، أ أو ب أو ج أو د، نعم هذا مستوى الأسئلة التي لدينا للزملاء الجديد. ولا يوجد سؤال هنا.

شخص غير محدد: فقط اقتبس ما قاله كلينتون، ماذا يعني نشر DNSsec؟

دان يورك: حسنًا، إنه مسجل. هيا. فأي هذه غير مسجل. حسناً؟ حسنًا. ماذا كان هذا جزءًا من ذلك. إلا ما ترمز كل من TPC وTPC.INT؟ مركز سياسة الانتقال، لجنة البرامج الفنية، أم الكابل عبر المحيط الهادي أم شركة الهاتف؟ لا يتعلق هذا بـ DNSsec. بل DNSsec/DNS. وهذا تلميح. إن كنتم تودون المساعدة في تحسين هذه الأسئلة فسيرغب روي فيها للجولة التالية. لذا، إن لم يعجبكم هذا، ساعدونا.

لذا، وإن لم يكن ذلك واضحًا، فما هو نطاق INT غير الموجود حاليًا؟ IPv4.int أم IPv6.int أم eurofish.int أم cto.int؟ ولا أعرف من أين أتي روي بهذه الأسئلة. حسناً؟ هذا أسهل. إلام ترمز do bit do في استعلام DNS؟ إيقاف DNSsec أم تشغيل DNSsec أم DNSsec صادر، أم DNSsec يعمل؟ ولن نتنازع في هذه. وسنعود إلى RFC. حسنًا.

إلا يشير الرقم 257 في سجل مفاتيح DNS؟ أ. مفتاح منطقة ونقطة دخول آمنة. ب. مفتاح تسجيل المنطقة في DNSsec. ج. الخوارزمية 257. أو د. CCLVII. ويمكن أن يكون هذا صحيحًا في سياق DNS. حسنًا.

رقم ستة. ما هي خوارزميات تجزئة NSEC3؟ [غير مسموع] واحد. [غير مسموع] 256. [غير مسموع] 384. أم Ghost R 34.11-94. ويمكن أن تكون هناك إجابات متعددة، تذكروا ذلك. روي، إن كنت تسمع. حسنًا. إلام ترمز CD بت في استعلام DNS؟ الخيار أ، قرص مضغوط، ب، تعطيل الفحص. ج. جهاز التشفير. أو د، لكافة محبي Windows وUnix وLinux والجميع، تغيير الدليل. محبي الكمبيوتر، نعم.

وسأعترف أنه إذا كنت سأخضع لهذا الاختبار فلن أكون متأكدًا من نجاحي في الإجابة على بعض الأسئلة. ولكن لدي الإجابات. لدي بعض الإجابات. وهي إجابات روي. حسنًا. إلام ترمز KSK؟ مفتاح الدخول الرئيسي. أم مفتاح إنهاء التحويل. أم مفتاح التحويل الرئيسي. حسنًا. بالنسبة لمن يستمعون عن بعد، لقد تمت الإشارة إلى أن روي، لم يقل "ماذا يعنيه في DNSSEC؟" وسيكون علينا --

إنه اختبار DNSsec، لذا، الخيار الأخير بالطبع هو Kappa Sigma Kappa، التي أعتقد أننا تحدثنا عنها. حسنًا. هل نحن مستعدون؟ ما هو عدد عناوين خادم ملف الجذر المختلفة هناك؟ الخيار أ، 12. الخيار ب، 13. الخيار ج، 24. الخيار د، 26. أرى أشخاصًا. أرى أشخاصًا ينظرون حولهم. ما هو عدد عناوين خادم ملف الجذر في DNS هناك؟ لا، كم عدد العقد هناك. ما هو عدد عناوين ملف الجذر هناك؟

أجل. لا تنظر في جهاز الكمبيوتر. حسناً؟ تم إغلاق الأجهزة. لا ذهاب هناك. هيا. لا، أي من نطاقات المستوى الأعلى لرمز البلد كان أول من ينشر DNSsec؟ أ.

بورتوريكو. ب. السويد. ج. الدانمرك. د. ألمانيا. وإن كنت أعرف روي، فربما تكون هناك خدعة ما في هذا. عندما تقولون نشر، فأنا سأقول عند التسجيل. حسناً؟

شخص غير محدد: هذه الأسماء ليست نطاقات ccTLD.

دان يورك: حسنًا. لذا، إن قرأت ذلك بدقة، فلاحظ أنها تقول "أي دولة لديها اسم نطاق، بين هلالين، كانت أولاً؟" لذا، أي دولة، وبالفعل، للأمانة، بورتوريكو ليست دولة. إذن. حسنًا. كيف نعمل؟ هل أنتم مستعدون؟ وهذا ما أردت توضيحه. برجاء التأكد من وضع اسمك على النموذج. هل فعلت هذا؟ لقد قمت بذلك بالفعل. حسنًا. أنا أنظر فيها، وأعتقد، شكرًا لك. حسنًا. حسنًا. لذا، تذكر، لديكم نقطة واحدة على كل إجابة صحيحة. حسنًا. لذا، هذه، خياراتنا، أي من نطاقات TLD هذه لا تنشر DNSsec؟ ما هي الإجابة؟ لا. لا. أ. لم تنشر الإكوادور DNSsec.

ب، الخيار ب، MA، المغرب. من المغرب هنا. نعم. 16 فبراير، وضعوا DS في ملف الجذر. مرحى. أحدث موقع لدينا. نعم. هو كذلك. حسنًا، ولكن لدينا تسجيلهم، ولكنهم ليس لديهم سجل DS، أليس كذلك؟ ليس لديهم مفتاح DNS؟ لديهم مفتاح DNS. أعلم ذلك. حسنًا، لا بأس يا رفاق. هيا. من يريد الوصول إلى الغداء. يوجد غداء قادم. حسنًا؟ لذا، القاعدة، حسنًا؟ والإجابة الأولى هي أ. اكتشفوا بنفسكم بالبحث في مكان ما.

حسنا، انظروا. لقد توصلوا. وهي موجودة. منذ متى وأنتم تعملون مع DNS؟ ألم تكتب برنامج ما؟ حسنًا. هذا أوندرج سوري من، لقد انتهي من الكثير بهذا. حسنًا [غير مسموع]، لا عذر هنا. حسنًا. تعالوا. حسنًا. انتظر حتى نصل هنا، أو ربما سن نصل إلى الغداء أبدًا. حسنًا.

ماذا فعلت TPC وTPC.INT؟ هل يعرف أحد هذا؟ هل أي شخص هنا عندما كانت TPC.INT موجودة؟ حسنًا، لا بأس. لقد قمت بتشغيله. حسنًا، فماذا هي الإجابة؟ ماذا؟ د. شركة الهاتف. ربما كنت سأحل هذه بصورة خاطئة. حسناً؟ ليست لدي فكرة عن هذا. فهذا كان قبلي. حسنًا.

ما هو نطاق INT غير الموجود حاليًا؟ ما رأيكم؟ أ. ما رأيكم؟ د؟ الإجابة ب. ip6.int ليس موجودًا حاليًا. فبوضوح، eurofish.int حقيقي. عليكم لوم روي، حسنًا؟ نعم التالية. إلام ترمز KSK؟ لا يمكنني الانتظار حتى معرفة هذه. الإجابة هي؟ كم عدد الأشخاص الذين يقولون أ؟ ب؟ ج؟ د؟ الإجابة د. DNSsec. ابحثوا عنها في RFC إن كنتم لا تصدقوني. حسنًا.

التالي. حسنًا؟ إلا يشير الرقم 257 في سجل مفاتيح DNS؟ أ. صحيح. في الواقع، مفتاح المنطقة ونقطة التأمين الجانبية. ما هي خوارزميات تجزئة NSEC3؟ كذلك. لذا، يقول روي أ فحسب، وأولافور يقول أنه محق. أعتقد أن أولافور كتب RFC في NSEC3، لذا، فهو يقول هذا، وأعتقد أن هذا مؤكد. لذا، الإجابة هي أ، هل يمكنني العودة لشريحة؟

أجل. حسنًا. لكن هذا الخيار كان أ. حسنًا. حسنًا. لنتابع. رقم سبعة، إلام ترمز CD بت في استعلام DNS؟ الإجابة هي؟ ماذا؟ ب. نعم. تعطيل الفحص. هذه هي الإجابة الصحيحة. إلام ترمز KSK في DNSsec؟ إلام ترمز؟ ستكون هذه أمنية في أماكن أخرى من المكان هنا اليوم، أليس كذلك؟ حسنًا. في مكان الانعقاد، لا يوجد شيء مماثل. إنه مفتاح الدخول الرئيسي. الاختيار أ.

حسنًا. ما هو عدد عناوين خادم ملف الجذر المختلفة هناك؟ لا يمكنني الانتظار حتى معرفة هذه. ج؟ ج؟ د؟ حسنًا. كم عدد الأشخاص الذين يقولون أ؟ حسنًا. كم عدد الأشخاص الذين يقولون ب؟ كم عدد الأشخاص الذين يقولون ج؟ أوه، انظروا. كثير من هذه. كم عدد الأشخاص الذين يقولون د؟ حسنًا. كان لدينا مجموعة من مشغلي تسجيل خادم الجذر. والزملاء من RSSAC هنا. لذا، لماذا هي ج؟ هذا صحيح. هناك 13 لديهم عناوين IPv4 وفقط 11 لديهم عناوين IPv6. ماذا، جيم؟

أوه. وماذا إذن؟ هل تقدم لي الإجابة الصحيحة؟ هل تقول أن الإجابة الصحيحة هي 25؟ حسنًا، لقد احتفظوا بالقديمة.

لارس–جون ليمان: فهي إذًا 27، لأن [غير مسموع] لا تزال [غير مسموع]. بالفعل.

دان يورك: وللجميع الجدد هنا، نحن هذا العبقري، نعم. حسنًا. سأوافق على 24. 24 صحيحة، والآن. حسنًا، 26، لا بأس؟ بسبب. حسنًا. سنوافق على إجابة روي، ولوموا روي، فهو ليس هنا. إنها 24، أليس كذلك؟ أنا أختر ج، إن كنتم تعترضون، فتحدثوا مع روي. نعم، بالتحديد. لذا، أي دولة كانت أول من ينشر DNSsec؟ بورتوريكو، أم السويد أم الدنمارك أم ألمانيا؟ وأرى، لقد قدمتها قليلاً، حسنًا. ما هي الإجابة؟ ب. السويد.

شخص غير محدد: عذرًا. أليست الدانمارك؟

دان يورك: ماذا؟ أوه، لقد كانت محاولة للمزاح، فهمت. حسنًا. حسنًا. دعونا نرجع إليها. لذا، ما عدد الأشخاص دعونا نبدأ بهذا. ما عدد الأشخاص، وعليكم إضافتهم جميعًا، فيجب أن يكون لدينا 10 نقاط إجمالي هذه المرة. وبالفعل، لم نقم بأي إجابات متعددة. كان روي يتباطأ قليلاً. حسنًا. حسنًا. دعونا ننتهي سريعًا للذهاب إلى الغداء. ما عديد الأشخاص الذين أجابوا إجابات صحيحة؟ أو واحد فقط، أليس كذلك؟ لا، دعونا نبدأ في الأعلى. أي شخص.

لا، لست أريد البدء في الأعلى. لنبدأ عند خمسة. ما عديد الأشخاص الذين أجابوا خمس إجابات صحيحة؟ على الأقل خمس. على الأقل خمس. ما عديد الأشخاص الذين أجابوا ست إجابات صحيحة؟ سبعة؟ ثمانية؟ تسعة؟ أعتقد أن لدينا رابط بين أوندريج وأولافور. حسناً. حسنًا، شكرًا لكم جميعًا. سنشكر روي على القيام بهذا، وإذا كنتم ترغبون في المساعدة في الاختبار التالي، فنتطلع إلى مساعدة الأشخاص في ذلك أيضًا. روي يحب التعقيبات.

حسنًا، بهذا، نحتاج للتوجه للغداء. جولي؟

جولي هيدلوند: أجل. لذا، فقط للتذكرة مرة أخرى، عليكم إحضار البطاقات. فأنتم تحتاجون لبطاقة لتناول الغداء. وهناك بالفعل مدخل واحد إلى منطقة الغداء. حسنًا، تحاط الجوانب الثلاث الأخرى بالماء، لذا، أفترض أنكم يمكنكم السباحة، ولكن حينها ستكون البطاقة مبتلة، وربما لن تبقى صالحة.

دان يورك: وإذا لم تحصل على بطاقة، إن أتيت لاحقًا ولم تحصل على واحدة، ولكنك تريد الانضمام لنا على الغداء، فيمكنك مقابلة أندرو وهناك بضعة أخرى.

جولي هيدلوند: ولكن بالأساس، يجب أن تكونوا هنا جميعًا كامل الوقت منذ الصباح، حتى تحصلوا على الغداء. لذا، عليك اتباع الخريطة على الجانب الآخر من بطاقتكم وسيكون هناك من يرشدكم، ولكن بأي سعر، حظًا سعيدًا. سنراكم قريبًا.

دان يورك: مجرد ملاحظة. لن يتم إغلاق هذه القاعة، لذا، ربما تريدون إحضار شيء معكم وما إلى ذلك.

ومع احتفال الحشور هناك، كما يقول باول، فلا أحتاج لسترتي، لذا، هذا جيد. لذا، أعضاء اللجنة، التي ستتكون ممن؟ دان، هذا أنا. جيوف هيوستون وجيم جالفين وأولافور وأوندريج. لماذا لا تأتي وتجلس في المقدمة؟ لذا، إن أردت الجلوس، فيمكنك إما الجلوس بجواري، أولافور، أو يمكنك الجلوس هناك. ولكني أرى، حسنًا، اجلس هناك، حتى يمكننا حينها.

جولي بجوار كاثي، ولكن، من لدينا هناك؟ لا أعرف. حسنًا، يمكن لإبرهارد أن يتحرك. نعم. وجيوف، إن كنت تريد التقدم هنا، فيمكنك ذلك والانضمام لنا أيضًا. كما يمكنكم الجلوس. ها نحن ذا. حسنًا، مهما يكن، فهي حقيبة رائعة. ولست متأكدًا من صاحبها.

لا، سنضع أوندريج عندما يعود. سيجلس حيث كانت سارة تجلس. هذا لي، روبرت. هذا لي، لكن يمكنك الانتقال إن رغبت. حسنًا، لأني سأجلس هنا طوال الوقت، ولكن يمكن أن تتحركوا. كل شيء جيد. فذراعكم تعمل بصورة جيدة إن قمتم بهذا. لديك معطف رائع خارج الصفقة. أوه، يمكنك الجلوس هناك. لم نعرف من كان، لذا فقد بدأنا بك.

حسنًا. مساء الخير في جلسة العصر هنا في ورشة عمل DNSsec. ونحن نعود إلى مقاعدنا، إن كنتم تجلسون في مقعد مقابل الحائط أو في مكان آخر، فمرحبًا بكم للقدوم

والانضمام إلينا على الطاولة. على الرحب و السعة. يمكنكم القيام بذلك. تتمثل الميزة الجانبية في الانضمام إلى الطاولة في حصولكم على مقبس يمكنكم استخدامه، إن أردتم للكهرباء. كما أنكم تحصلون على ميكروفونات لطيفة مثل ذلك والذي يمكنكم استخدامه عند رغبتكم في الحديث عن المشكلات المطروحة هنا.

بالرغم من أن زملائي في اللجنة أخبروني أننا سيكون لدينا نزاع بين السيدين الكبيرين على يساري هنا. ومع ذلك، فكلاهما طويل وضخم، ويمكن أن يكون الشجار مثيرًا. لذا، ربما نضعهم في المنتصف هنا، ونمنح كل منهم منشارًا كهربيًا ونرى ما يحدث.

سيبدأ وارين في أخذ الرهانات. حسنًا. لست متأكدًا ما إذا، هل لدينا أي شخص من المغرب يمكنه أن يخبرنا؟ هل مسموح بالمنشار الكهربي هنا؟ هل هو شجار؟ لا، السيوف، ربما. لا أعرف. ماذا نفعل؟ لست متأكدًا. الخناجر. الخناجر، نعم. سنذهب إلى السوق ونرى ما يمكنه اختياره. حسنًا.

وبصورة جدية، شكرًا لكم جميعًا على العودة. نريد أيضًا أن نقدم جولة كبيرة من التصفيق والشكر لكل من Afilias وسارة وSIDN. لا، قلت سارة. Afilias وسارة وSIDN ودين. دين. كما أشكر كايلي يورك في دين، الذي كان من رتب الأمر، وفعل كل هذا. وهو الرئيس التنفيذي للتسويق، وما إليه، هناك ولذا، فقد رتب هذا. مع ذلك، لا توجد علاقة بيننا، بالرغم حتى من أننا كنا في نيو هامبشاير. عالم غريب. ها نحن ذا.

أنتظر فقط ظهور الشرائح في غرفة Adobe. حسنًا. نحن جميعًا على ما يرام. لذا، أريد بدء الجلسة. تتعلق هذه الجلسة كلها بموضوع DNSsec وتشفير المنحنى الإهليجي وقد حصلنا على بضعة قطع مختلفة هنا. وسأرى الشجار الذي نتحدث عنه حول منذ قليل هنا. كذلك، فأنا أساهم بالقليل فقط وكذلك داني جرانب بالفعل في البداية. فلننتقل إلى الشريحة الأولى.

أسباب أننا نستخدم خوارزميات DNSsec، لأني أعرف أن لدينا بعض الزملاء الأحدث هنا، كما نعتقد، كما أننا نستخدمها لإنشاء المفاتيح للتسجيل ونستخدمها في توقيعات DNS وكذلك في سجلات DS لإنشاء سلسلة الثقة العالمية، وكذلك في التحقق من الصحة. وهي هي النقاط الي علينا التعرض لها عند النظر في تغيير خوارزميات DNSsec. الشريحة التالية.

لذا، عند النظر في سجل IANA الحالي، هناك نطاق كامل من الخوارزميات القائمة. وكما قد يطرح جيوف هيوستون عند الحديث عن نسبة صغيرة للغاية عن هذه المستخدمة بالفعل. ففي الواقع، فقط نسبة صغيرة للغاية تستخدم بالفعل. ولكن هذه هي الخوارزميات المتوفرة الآن. الشريحة التالية من فضلك.

وهناك اثنان أحدث في، وإذا قمنا بتوسعة تعريف الأحدث ليعود إلى حوالي خمس سنوات، أو ستة، كما أعتقد، إذا كنا قريبين من ذلك، فالاثنين هما ECDSA وGhost. الآن، كان لدى ECDSA اعتماد قليل حتى حوالي أربعة شهور، عندما قامت CloudFlare بتشغيلها وإضاءتها للسجلات التي كانت هناك. الشريحة التالية الآن. سنتحدث عن الأخرى في دقيقة.

لذا، الأسباب التي نهتم بها هي بعض مما تحدث عنه داني سابقًا. أسرع، ربما أسرع كثيرًا في التسجيل وكذلك في التحقق من الصحة. ويعتمد هذا على الوضع، ويمكن وجود حجج في أي اتجاه. مفاتيح وتوقيعات أصغر. وتشفير أفضل. كما سأذكر النقطة الأخيرة وهي نقاط الضعف المحددة لي.

فجزء مما تعرفون أنه مسؤوليتي نحو مجتمع الإنترنت هو المساعدة في تسريع اعتماد DNSsec والعمل على الدفاع عن محاولة استخدام الناس لها. وأحد نقاط اضعف المحددة، التي لدينا الآن هي أن هناك جزء كبير من مجتمع الأمن ينظر في كيف يمكننا الابتعاد عن مفاتيح RSA 1024 بت.

وعلى وجه الخصوص، ينظر مجتمع برامج تصفح الشبكة في إيقاف كل دعم لشهادات TLS، يكون أقل من 2048 بت. الآن، يمكننا أن نجادل مع مجتمع برامج تصفح الويب، فيما يتعلق بأن الطريقة التي نقوم بها بالأمور مختلفة، ولدينا مفاتيح ZSK لثلاثة شهور أو شهر واحد أو الأمور الأخرى المشابهة. كما يمكن أن تكون لدينا حجج حول سبب أنه مناسب، ولكن في نهاية الأمر، هناك تصور عام أن RSA 1024 بت سيء للغاية، لذا علينا التخلص منه. ومن وجهة نظر أمنية، هذه حجة مناسبة.

لذا، فقط للتطور فيما يتعلق بجعل الأمور أكثر أمنًا وثقة في كل من DNS وDNSsec، نريد الابتعاد عن هذه المفاتيح والمنحنى الإهليجي الذي يمثل حاليًا طريقة النظر في الموضوع. الشريحة التالية من فضلك.

كما ذكرت، هناك هذه الجوانب التي نتعامل معها عند نشر الخوارزميات الجديدة. وعلينا التفكير في التحقق من الصحة، كما أن علينا التفكير في التسجيل ومشغلي استضافة DNS الذين سيقومون بهذا. كما أن علينا التفكير في السجلات وقبول سجلات DS. وعلينا القيام بالسجلات والمطورين وكافة هذه الأمور. الشريحة التالية من فضلك.

من ناحية التحقق، لقد نظرنا في هذا وقلنا أن المحلل يجب تحديثه بالخوارزميات الجديدة لتنفيذ التحقق. لذا، فنحن نتطلع إلى طرح خوارزميات جديدة، وعلينا طرح هذا في كافة البرامج الموجودة. كما سمعنا بالفعل من المكاتب التي لم يتم تحميلها، عن عدم وجود ذلك لديهم. فكيف تذهب وتقوم بهذا؟

الجزء الآخر الذي حددناه في الماضي أيضًا، هو أن RFC 4035 تنص على أنه في حالة عدم دعم المحلل لأي من الخوارزميات، فيجب التعامل مع المنطقة كما لو أنها غير مسجلة. حسنًا، سأقوم بذلك. وبهذا، فقط بسبب أننا نستخدم DNSsec مع خوارزمية مختلفة وآمنة، ونتعامل مع المنطقة التي يتم التعامل مها كما لو تكن مؤمنة من DNSsec على الإطلاق. الشريحة التالية من فضلك.

من ناحية التسجيل، يحتاج البرنامج على الخوادم المعتمدة للتحديثات بالطبع. ويمكنكم الاطلاع على الأجزاء الأخرى هنا. كما أن علينا تحديث هذا، وعلينا الذهاب وتغييره. كما يمكن أن تكون هناك تأثيرات أثناء الانتقال في الدور من خوارزمية إلى أخرى. وهناك فترة زمنية متاحة. الشريحة التالية من فضلك.

السجلات، كما ترون هنا. حيث يقبل البعض سجل DS مع بعض الخوارزميات فحسب. كما أننا دخلنا في هذا التحدي الذي لا نعرف من الناحية النظامية ما إذا كانت سجلات الخوارزميات ستقبله. كذلك، ليست هناك طريقة لمعرفة ما الذي ستقوم به الخوارزميات بالضرورة عند تقديم المفاتيح بطرق محددة. وأحد الاقتراحات كان أن نقوم بتحديد

العناصر هنا. ولا أحتاج، سأقرأ هذا حيث أني هنا للمشاركين عن بعد، ولكني حدثت منشور EPP. فهل هناك طريقة يمكننا بها الذهاب وتحديث ذلك؟

هناك أيضًا سؤال متواصل حول لماذا تحتاج السجلات لفحص نوع الخوارزمية؟ وكان لدينا بعض النقاض حول هذا في الماضي. الشريحة التالية من فضلك. كما أننا يمكننا الدخول في نقاش حول هذا، لكن على أي حال.

لدى بعض أمناء السجل واجهات ويب تقبل فقط بعض الخوارزميات. وكان هناك مثال على أحد أمناء السجل، يجب أن يبقى دون اسم، ولكن ربما يكون صاحب عمل وارين. حسنًا. كما كان هناك، بكل جدية، في نطاقات جوجل، لقد قاموا بالأمر الصحيح. وهذا هو الموقف قبل سؤال شخص ما عن ECDSA حيث كانت هناك قائمة ببضعة خوارزميات فحسب، ثم الشريحة التالية.

بعد ذلك، كان لديهم مجموعة كاملة من الخوارزميات هناك. وستلاحظون أيضًا أنهم وضعوا الأرقام بجانب الخوارزميات في هذه الواجهة، وهو ما يتضمن قليل من الفضول لأن لدينا حالات سيقوم مشغلو استضافة DNS بإنشاء سجلات DS. وإذا كان الشخص الذي كتب مواصفات سجلات DS، فعليكم لومه على هذا.

على أي حال، سيقدمونه لكم مع عدد، ولكن ليس الخوارزمية، وأمور أخرى ستقدم لكم الخوارزمية ولكن ليس العدد. لذا، بالنسبة لأمناء السجل، تعتبر أذكى طريقة للقيام بهذا هي عرضها حتى يصبح الأمر أقل لبسًا على الناس. كذلك، المناقشات الأطول، التي أعرف أن أولافور وجاك وآخرون ينظرون فيها إلى طرق للحصول على هذا النوع من المستخدمين خارج المساحة لإدخال هذا.

لكن على أية حال. الخطوات التالية. لذا، مرة أخرى لقد مررنا بهذا، لماذا يحتاج أمناء السجل للقيام بهذا. يتعين عليهم فحسب قبول سجلات DS، إلا أننا نعرف أن لدينا هذه المناقشة حول ذلك تصل إلى واجهات المستخدمين، للتحقق من تقليل مشكلات الدعم، وهذا النوع من الأسئلة. الشريحة التالية.

لذا، بالنسبة للمطورين، يتمثل التحدي بالطبع في أنه في حالة إخبار شخص ما، ومنح الأشخاص قائمة بالأمور للتحقق منها، فسيتم إخبارهم بالتحقق من الحدود والقوائم. لذا، فهي ليست قائمة، حسنًا، عليكم القيام بها. ويتمثل التحدي بالطبع في أنه في العديد من الأوقات مع صياغة البرامج وعدم تحديثها عندما تكون هناك إضافات جديدة في الخوارزميات. لذا، عندما ننظر في الخوارزميات الجديدة على قائمة IANA، فالعديد من البرامج هناك التي تتحقق من الخوارزميات الحالية لن تقوم بتحديث القائمة حتى نذهب في وقت ما ونطلب ذلك منهم.

الشريحة التالية. هناك نوع من إعداد المرحلة للنقاش مع نظرنا في كيف يمكننا إضافة خوارزميات جديدة. فكيف نطرح هذا الأمر؟ نحتاج للنظر في كيف يمكننا مساعدة الناس على الفهم؟ وكيف نساعد في دعم قيمة هذه الخوارزميات الجديدة؟ وكيف نذهب ونبدأ القيام بتفعيل هذه التغييرات؟ كما أن هناك جزء مما نتحدث عنه هنا ونطرحه، هذه اللجنة، مع تحدثنا عن المنحنى الإهليجي.

كذلك، نريد أن نذهب ونرى ما علينا القيام به لحدوث هذا، وطرح DNSsec يكون حتى أكثر أمانًا. ومن ثم أعتقد أن هذا لي. وأعتقد أني كنت سأقترح أن يتحدث جيوف قليلاً عما يراه في طريق DNSsec، التالي.

وإذا كانت لديكم أسئلة في أي وقت، إذا كانت هناك نقاط محددة للشخص العارض، الرجاء سؤاله وطرحها. وإذا كان هناك نقاش أطول، فربما يمكننا الانتظار حتى انتهاء اللجنة. لكن، إذا كان لديكم سؤال توضيحي محدد، فيسعدنا تلقيه.

جيوف هوستن: لا توجد أسئلة؟ حسنًا. سأبدأ إذن. وأنا جيوف هيوستون، وأعمل في APNIC. وأقوم بقدر كبير من العمل في القياس. وأحد جوانب القياس هي بالفعل قياس DNSsec. وفي هذه الحالة، أريد أن أنظر في مستوى الدعم في ECDSA على جانب المحلل. لذا، أنا أنظر في الخوارزمية التي ترون لتسجيل المناطق وما إلى ذلك. ليس هذا ما أتطلع إليه.

فأنا أتطلع إلى المحللين. وفي حالة تسجيل منطقتكم لدى ECDSA P-256، وهي خوارزمية التشفير رقم 13، فهل يتمكن الزملاء بالفعل من استخدام هذه الخوارزمية ومعرفة ما إذا كانت هذه المنطقة آمنة؟ الشريحة التالية.

لذا، الجميل في الموضوع أننا عندما سمعنا هذا الصباح، تم إخبارنا، ولم تكن لدي مشكلة في الاعتقاد بذلك، قوة ECC تكمن في الواقع في وجود حسابات أكثر وقدر أقل من وحدات البت. لذا، لم أقم بخطة نقطة المياه من الأعمال بحجم الأرض، ولكن بقدر ما يمكنني أن أرى وما قيل لي، فإن 256 بت من ECC تعادل 3072 بت في RSA. وهذا بالتأكيد أكثر كثافة من حيث قدرات التشفير.

هذا مهم في DNS لأن مواصفاته الأصلية تقول أنه بمجرد الحصول على رد أكثر من 512 بايت، يتم إيقاف كافة الوحدات. الآن، مع ذلك، يمكننا فعل أكثر من هذا. ولكن المثير للانتباه هو أنه بمجرد الوصول إلى أكثر من ألف مجموعة ثمانية والتوجه نحو الرقم السحري 1500، لا يمكن لبعض المحللين التوصل إلى الإجابة. وبعد ذلك، شاركتم في المشكلة بالكامل بمجرد حصولكم على أكثر من 1500 مجموعة ثمانية، وحدوث تقسيم UDP. ومرة أخرى، هذا هو الكابوس الخاص بنا.

كذلك، إذا كنتم تتولون تشغيل الإصدار السادس وتقسيم UDP، فعليكم الدعاء لأنه لن يساعدكم أي شيء آخر. ولذا، هناك مشكلات فعلية في حجم الرد على التقسيم. لذا، تفضل الخوارزمية الأصغر، مع تساوي كافة الأمور الأخرى. الشريحة التالية.

لذا، هناك نوع من الأمثلة في ECDSA، بالفعل نفس السؤال المسجل في ECDSA، 527 مجموعة ثمانية. وأنا تقريبًا تحت القيمة السحرية 512، بالتحديد نفس الأمر، RSA 937. وهذا نموذجي للغاية. نعم التالية.

إذن لننتقل إلى ذلك، حسنًا؟ ليس هناك مشكلة. لكني أكون مثل أني يمكنني الذهاب وتسجيل الأمور في ECDSA، ولكنك الشخص الذي عليه قبول أي منطقة مسجلة. وبهذا، فالسؤال الحقيقي هو إذا قمت بهذا، فل ستصدقونني؟ ولذا، أنا أنظر بالفعل فيما إذا كنت سجلت باستخدام ECDSA، وأي من المحللين سيتحقق من صحة التوقيع؟ فمن يقدر على دعم هذا البروتوكول؟ نعم التالية.

لذلك، نستخدم إعلانات جوجل لقياس الشبكة من جانب المستخدم. وتعتبر هذه الإعلانات مفيدة للغاية. كما أن الأمر بسيط للغاية. فهمي تقوم بما نقوم به عادة، تبحث في URL. الآن، يعتبر URL نوعًا ما خاص لأن لديه مكون DNS، وبعدها مكون ويب. كما أن مكون DNS تحت سيطرتي. والاسم فريد بالفعل وكل اسم يستخدم مرة ومرة واحدة فقط، كما أن جوجل متميزة بالفعل. لذا، إن كنتم ستقومون بإعلان غير ملهم بصورة كبيرة وساذج ولا يترتب عليها أي إيرادات، تقدم جوجل لكم اهتمامًا أكثر لأنهم يريدون بالفعل عرض هذا الإعلان للحصول على قدر من النقود من عملائهم. لذا، فالأسوأ، بالنسبة للإعلان، كلما زاد عدد المرات، زاد تأثير الإعلان. جيوف السعيد.

لذا، في هذه الحالة ما يحققه الإعلان هو وجو نص صغير في الداخل يتضمن خمسة عناوين URL. اسم فريد للغاية، بحيث تتصادم هذه الاستفسارات مع سلطتي في خوادم الاسم في كل مرة يحاول أحد المستخدمين حل هذا. ولدي عدد منها في العالم. لذا، كما ترون هناك، أنا أحاول السيطرة على الاختبارات. والسيطرة المطلقة ليست مسجلة في DNSsec على الإطلاق. هل يمكنكم حل هذا الاسم؟

الاختبار التالي، التوقيع المستند إلى RSA. فهل ستحصلون عليه؟ الاختبار الثالث، أنا مهتم بالفعل بما يحدث إذا قدمت لك شيئًا معطل بصورة متعمدة. وبعبارة أخرى، يجب ألا تثق بهذا الجزء من DNS. فالتوقيع لا يعمل. فعليكم قبول فشل الخدمة والتعايش مع هذا. ولن يحل هذا الموضوع. كما أكرر هذين الاختبارين يستخدمان بالضبط نفس الآلية، ولكن هذه المرة مع ECDSA P-256. نعم التالية.

لذا، هذا ما يبدو عليه الإعلان بالفعل من حيث URL. وهناك بعض الأمور الفريدة هنا، وبعدها هناك، إن كنتم ستقومون بهذا، نوع من المسميات العامة التي يمكنني ربطها معًا، وهذه هي خمسة عناوين URL مختلفة. لذا، إن رأيتم الإعلان، فهذا ما سيقدمه المتصفح ويبحث ويحاول ويحل أسماء النطاق الخمسة المميزة في الخلفية. نعم التالية.

الآن، يمثل DNS، هذه رؤية بسيطة وهي واقعية. لذا، فالرؤية البسيطة مثيرة بالفعل، وسهلة بالفعل. وقد طرحت سؤالاً، وتم توجيهه إلى الخادم، قبل أن يعيد الخادم الإجابة. نعم؟ استعلام واحد ورد واحد. بالنسبة للتحقق من DNSsec، يتضمن الأمر قدر أكبر

قليلاً من العمل، ولكنه لا يزال بسيطًا، حيث تطرحون السؤال، وأرد عليكم بإجابة موقعة. كما أنكم تتحققون من هذا أولاً، وربما يكون الترتيب مختلفًا، ولكنكم تسألون عن سجل DS، من الأصل، وبعدها تطلبون مفتاح المنطقة للفرع، سجل مفتاح DNS.

لذا، ما علي أن أراه إذا كنت أتحقق من صحة المحلل، أني يجب أن أرى هذه الاستعلامات الثلاثة وليس واحد فحسب. نعم التالية. لذا، هذا ما يجب أن أراه، اليس كذلك؟ وأرسل لك هذا، يجب أن أرى الاستعلامات الثلاثة لكل من هذه السجلات. نعم التالية.

كما أن DNS هي العمل المتميز في الالتفاف. فهو ليس هندسيًا، بل عشوائي. ولا شيء مباشر عند النظر في أخطاء DNS. كما أن هناك مجموعات تابعة، وتكرار للاستعلامات. كذلك، سيحدث أي شيء يمكن أن يحدث. وهناك ربما سلاسل استعلامات هناك، ولكنها لا تزال تتغير نظرًا لعدم وجود TTL في أي استعلام. لذا، ربما لا يتحدث نصف المرسلين في DNS إلى النصف الآخر من DNS لأي سبب مهما يكن. نحن لا نعرف. لذا، فكل شيء لديه وقته الخاص. وعندما طرح سؤال، فالسؤال يتكرر فحسب. نعم التالية.

وهذا مثال بسيط للغاية على التكرار. عندما طرح العميل سؤال وطرح كافة المحللين الخمسة أسئلة أرسلتها إلى العميل الأصلي. بعد ذلك، ينظر المحلل الأول في شيء يعمل من خلال ISP لهذا العميل، وحقيقة أنه كان هناك سجل واستعلام مفتاح DNS، وبعدها تميل DS لقول أنها تتحقق من الصحة. التالي هو جوجل. وهذا هو المحرك التابع لجوجل. DS، مفتاح DS، DS، DNS. لم تعجبني أو DS. لذا، فهذا غريب قليلاً. وهناك تابع آخر على بعد عنوانين، 145، والذي يبدو أنه يعمل في مجموعة مع التابع الأول، لأنه يتضمن مفتاحي DNS المفقودين، أليس كذلك؟

ولكن بعد ذلك، يشارك محلل ISP الثاني أيضًا، ويسأل مجموعة من الأسئلة، وفقط من بينها، هناك محلل جوجل يسألني عن سجل DS. لذا، إذا لم أعرف بالفعل أن عناوين جوجل الثلاثة كانت جزءًا من نفس العقل، فذلك سيبدو غريبًا بالفعل. وإذا لم أعرف نوعًا ما أن هؤلاء المحللين المائتين كانوا جزءًا من نفس ISP، فستتساءلون عن ما يجري هنا.

لذا، بدلاً من وجود ثلاثة استعلامات وثلاث إجابات، كما ترون، فهناك 12 استعلامًا و12 إجابة، وهذا نوع من الصعب فهمه، ولكن يبدوا هذا على أنه تحقق من الصحة. نعم التالية. وفي هذا بعض الأسباب، عليكم البحث عنها في الشرائح. والسبب بالمناسبة أن هناك العديد من الاستعلامات هو أن هذا مسجل بصورة خاطئة. لذا، عند إرسال المحلل الأول، 25522468، ردًا، فلا يمكنني القيام بهذا. فهو لا يقول أني لا يمكنني القيام بهذا لأنه لا يوجد، لا يمكنني القيام به في DNSsec.

فهو يقول ببساطة، "أنا، لقد فشل الخادم." وهو ما يتضمن رسالة بالمحاولة مرة أخرى. ولذا، يحاول المستخدم استخدام جوجل. وتقول جوجل "حسنًا، إذا فشل الخادم،" لذا، يصاب بالإحباط. فهي تقول أن الفشل في DNSsec مؤسف لأنه يتسبب بالأساس، ليس مجرد عاصفة استعلامات ولكن يتسبب في الكثير من الاستعلامات. نعم التالية.

لذا، ECDSA. كيف يمكننا النظر في عدد الزملاء الذين يقومون بهذا بالفعل؟ والأمر الأول بسيط للغاية بالفعل، وهو بالأساس الإحصائيات. لذا، لقد قمت بعدد عدد الاستعلامات الرئيسية في DS وDNS التي حصلت عليها من RSA، وكذلك نفس العديد للاستعلامات التي أحصل عليها من ECC. نعم التالية. لذا، فقد عمل هذا على مدار 45 يومًا، واختبرت 765 مليون شخص. وكانت الإعلانات رائعة. حيث تصل جوجل إلى الكثير من الناس بسرعة بالفعل. لذا، هناك 765 مليون شخص، 27% منهم مع DNSsec يتحققون من الصحة في RSA. وقد رأيت هذه الاستعلامات. هذا عدد كبير. كما ستتوقف V6 من هذه الأعداد.

دان يورك: لذا، جيوف، نحتاج للمتابعة.

جيوف هوستن: المتابعة؟ حسنًا. 23% ،ECDSA، لذا فهذا أقل قليلاً. نعم التالية. والوقت يمر، لذا، سنمضي بسرعة أكبر قليلاً. لذا، بالأساس، ما يبدو أن واحد من خمسة يمكنهم تنفيذ RSA لن يمكنهم تنفيذ ECDSA. نعم التالية.

الآن، واحد من خمسة أفضل مما كان. ففي سبتمبر 2004، كان واحد من ثلاثة يمكنهم تنفيذ RSA لا يمكنهم تنفيذ ECDSA. ولذا، يبدو أننا نتحسن قليلاً حسب الإحصائيات. نعم التالية.

لذا، سأنتقل الآن بمزيد من التفصيل وأرى إن أمكنني تتبع هذا. نعم التالية.

فما أنظر فيه بالفعل هو ذلك الاستعلام المهم الذي يقول، "هذه هي ECDSA." وهذا خارج سجل DS. نعم التالية.

لذا، إن نظرتم في الكلمات التي قالها السابقون. نعم التالية.

دان يورك: نعم التالية.

جيوف هوستن: ما زلت أمضي بسرعة. فالمهم بالفعل هو سجل DS. نعم التالية.

لذا، الآن، التالي، إنها بالفعل حقيقة أني عندما أرى شيئًا في DS، لا أعرف، أتركه. نعم التالية.

لذلك، هذا يأخذني إلى الإجابة الفعلية. وباستخدام مستوى أكثر تفصيلاً من المشاركة، يستخدم واحد من بين ستة عملاء المحللين الذين يدعمون RSA وليس ECDSA. نعم التالية.

ربما يكون هذا الملخص. نعم التالية.

هل هي فعالة؟

دان يورك: يمكنكم ترك هذا الملخص هناك للحظة.

جيوف هوستن: لا، هذا كان الملخص. حسنًا. لذا، لننتقل بالفعل إلى أمر ما. إن كنتم تعيشون في دومينيكا، حيث يوجد 98% فشل في ECDSA. وهذا سيء للغاية بالفعل. إن كنتم تعيشون في نيوزيلندا، حيث يوجد 70% فشل في ECDSA مقابل RSA. وهذا سيء للغاية بالفعل. إن كنتم تعيشون في جنوب أفريقيا، حيث يوجد 75% فشل. وهذا سيء للغاية بالفعل.

لذا، عندما يكون هناك نوعًا من الفشل بنسبة واحد من ستة، فهذا ليس موحدًا، بل يعتمد على الحالة. التالي، إن كنا نصل بالفعل إلى النهاية. لماذا يجري هذا؟ ونحن قادرين بالفعل على تحديد المحللين الأفراد. وما نجده بالفعل هو أن أغلبية المحللين الذين لا يدعمون ECDSA يعملون عبر شركات الهاتف التي تقدم خدمات البيانات للهواتف المحمولة.

وما يبدو هو أن قطاع المستخدم المحدد يخرج الأمور من الصندوق، وينزع الشريط اللصق، ويقوم بتشغيله. كذلك، ليس لديهم أدنى فكرة عما هو موجود في الصندوق. كما أن المحللين الذي يعملون هذا يساهمون في معدل الفشل. وإذا استطاع قطاع العمل هذا أن يفهم بالفعل تكنولوجيا المعلومات، فربما يكون لديكم مشكلات يتم حلها. وهذا كل ما بوسعي قوله. شكرًا.

دان يورك: شكرًا لك جيوف.

جيوف هوستن: وعذرًا، للتشغيل أكثر من 4 دقائق و54 ثانية.

دان يورك: شكرًا لك جيوف. وهذا، حسنًا. لا، هذا جيد ومثير حول جانب الاتصالات من هذا. حسنًا، جيم، هل تريد الحديث عن جانب السجل من هذا؟

جيم غالفين: إذن، نعم. شكرًا لك، دان. أنا جيم جالفن من Afilias، وبما إن الجميع هنا ربما يقدم لك نوعًا من الأخبار السيئة، أو الأخبار التي ترغب في أن تكون مختلفة. فأعتقد أني هناك لأقدم بعض الأخبار السارة، كما أفترض.

من وجهة نظر السجل، نحن بوضوح مشارك مهم في هذه المساحة لسببين، ولذا، هناك أمران سأتحدث عنهما. الأول هو أن على السجلات نفسها أن تكون مستهلكة للتكنولوجيا. وفي هذا الصدد، لأننا سجلنا نطاقات TLD، فعلينا العثور على هذه الحلول المتوفرة ولكن من المهم تذكر أن السجلات موجهة بالمتطلبات وهذه المتطلبات تأتي من مكانين. الأول هو المعايير، وهي قيد التطوير بوضوح، والمتطلبات في هذا الصدد. على أن لدينا قائمة بالتأكيد للخوارزميات السارية.

الجانب الآخر من ذلك هو أنه من وجهة نظر سجل وgTLD على وجه التحديد، لدينا طرف متعاقد مع ICANN ولذا، هناك متطلبات ناتجة عن السياسات من خارج ICANN لسوء الحظ، يتعين الالتفات لها. حسناً؟ ولكن بعيدًا عن هذا، في بعض الأحيان.

ولكن، كل هذه أخبار جيدة. وأعتقد أن هذه هي كل الأمور، التي تم تحديدها ببساطة، إن كنتم ستقومون، أو ربما قمتم بتلبية الاحتياجات أو المتطلبات الخاصة بتبديل الخوارزميات. وكسجل، وعلى وجه التحديد حتى نصبح مزود سجل كبير، فلدينا الكثير من العملاء المختلفين. فنحن الآن أكثر من 100 من حيث نطاقات TLD التي ندعمها. كما أن لدينا حاجة لأن نصبح مزود خدمات عامة ونقدم الخدمات عبر مجلس الإدارة.

أما النصف الآخر من المشكلة، أو من المساحة التي تساهم فيها السجلات، فيتمثل في دعم المشتركين وأمناء السجل، خاصة في مساحة gTLD. ويرجع ذلك مرة أخرى إلى أن لديكم مجموعة من المتطلبات، وبالتالي توجهكم هذه الأمور من جانب ICANN كطرف متعاقد. كذلك، توجد قواعد حول كيف يتعين أن تعمل الأمور، ولكن علينا السماح للمشتركين الذين لديهم أسماء النطاقات والذين لديهم خوادم DNS، والذين يريدون دعم الخوارزميات الأخرى بجانب RSA فحسب حاليًا، بجانب قدرتهم على طرح هذه سجلات DS في منطقة TLD، بحيث تتوفر للبقية، وهو ما سنكتشفه، على أن هذا لا يعمل بهدوء ولكنه سيعمل أفضل من الوصول هناك.

من وجهة نظرنا، لدينا ميزة لأننا نريد دعم الكثير من نطاقات TLD والكثير من النطاقات المختلفة. لذا، بالنسبة لنا، فإن القيود محددة قليلاً من حيث ما يطلب من أمناء السجل القيام به، ونحن نرغب في التعامل بأنفسنا مع أي خوارزمية. كذلك، سنقبل بالفعل أي من الخوارزميات المدرجة السارية، في المعايير الفنية، لأن هذه ليست متطلبات من جانب ICANN، ولكن متطلبات السياسة هي من يقيد هذا.

كذلك، يوجد نوع ما من قابلية التشغيل البيني لأمناء السجل، في أننا نأخذ سجلات DS، وليس السجلات الرئيسية. كذلك، تفضل بعض السجلات أخذ السجلات الرئيسية من المشتركين بحيث يمكن تحويلها إلى سجل DS لوضعها في منطقة TLD. لذلك، فأمناء السجل هم من يجعل هذه مشكلة. لكننا نأخذ فقط ما تقدمون، ونتمسك به، وطالما أنه متسق ذاتيًا وصالح، فنحن لا نهتم. هذا هو الخبر السار.

من ناحية أخرى، هناك سجلات تركز أكثر بوضوح أو ربما تكون أنواع فردية من سجلات TLD أو مزودي خدمات السجل التي تدعم فقط TLD واحد. وربما يكون هناك مجموعة متنوعة من مختلف أنواع القيود أو ما يمكنهم فعله، لذا، ربما لن يرغبوا في التعامل مع هذه الخوارزمية. لكني أعتقد أنكم ستجدون في مساحة gTLD، خاصة لمن يدعم معظمها، لن يكون لديكم الكثير من هذه الأنواع من القيود، والأمور التي تعمل بسهولة وبصورة مباشرة. وهذه ما يعمل معنا.

أعتقد باختصار، أن ما سنقوله هو أننا موجهون بالمتطلبات الخارجية، وليس المتطلبات الفنية. وطالما توجد التقنية، فنحن نؤيدها. أليس هذا صحيحًا؟ ولكننا موجهون بالمعايير ويجب إنجاز ما تقول. ومن المهم تذكر أنه كسجل، يتمثل موضعنا في المنظومة في أننا موجهون بالسياسات التي نلتزم بها عبر علاقتنا التعاقدية مع ICANN على وجه الخصوص.

كما أعتقد أن كافة هذه الأمور مشكلات قابلة للحل، لذا، فهذه أخبار جيدة. وبهذا، نريد أن نكون مشارك جيد وشريك مناسب لكافة هذه الأمور مع الناس. لذا، سأترك الأمر لبقيتكم حتى يصبح هذا سيئًا للمجتمع. شكرًا.

دان يورك: حسنًا. شكرًا لك، جيم. لذا، لقد سمعتني أحدد مرحلة ما علينا فعله لتغيير الخوارزميات. وقد سمعنا جيوف يتحدث عن حقيقة ما نراه من جانب التحقق، والجزء الأول من هذا. كما سمعنا جيم يقول أن السجلات ترغب في القيام بهذا إذا كان هناك دافع خارجي، إذا ذهب الناس وغيروا ذلك بصورة ما، والآن، سيكون لدينا أولافور الذي سيتحدث قليلاً عما يراه في هذه العملية، ويجب أن أقول فحسب أننا سنلخص هذا، مع أوندريج الذي سيتحدث عن، حسنًا، كل هذه أمور شيقة، ولكن لدي بعض الخوارزميات الجديدة للتعامل معها هنا، لذا، كيف يمكننا القيام بهذا؟

بعد ذلك، نريد فتح الباب للأسئلة وبعض الحوار، ولدي بعض الأسئلة لكني أتطلع لأسئلتكم جميعًا، أيضًا، لذا، أعتقد أننا سننتقل إلى أولافور الآن.

أولافور جوموندسون: شكرًا لك، دان. لقد نشرنا خوارزمية DNSsec جديدة سابقًا هذه السنة، عذرًا، السنة السابقة. وقد كانت سنة طويلة. كما أن هذا يتعلق ببعض الأمور التي اكتشفناها. وأعتذر إن لم يكن حديثي شيقًا كزملائي، داني هذا الصباح، ولا يمكننا جميعًا العيش بنفس مستوى المعايير المرتفعة.

دان يورك: أنتم تحققون التوازن بين كل منكم الآخر في السرعة، بالرغم من ذلك.

أولافور جوموندسون: أحاول أن أكون مهذبًا تجاه المترجمين. ولقد تلقيت صراخًا في البرازيل بسبب سرعتي في الحديث. حسنًا. إذن الشريحة التالية.

دان يورك: [غير مسموع] الشريحة التالية.

أولافور جوموندسون: حسنًا. نحن أول من يقوم بهذا على نطاق واسع. ونحن نعمل بكد شديد حتى نجعل الآخرين يتابعون قيادتنا لأننا نعتقد أن هذا هو الأمر المناسب لمختلف الأسباب التي وضحها الآخرون. إلا أن الدرس الكبير المستفاد من كل هذا هو نموذج تسجيل ICANN، والذي نسخه العديد من نطاقات TLD، وتم تقسيمه، لأن مشغلي DNS غير موجودين في هذا النموذج، وهم من يجب أن يتمكنوا من إدراج المعلومات بدلاً من المرور بقناة المشترك الرئيسية. الشريحة التالية.

حسنًا، يمكننا النظر في العرض البسيط بالفعل في DNS، والذي ربما يكون أكثر تعقيدًا مما يفهمه الكثير من العاملين على السياسات بالأعلى. هناك خوادم [غير مسموع] تشكل المحللين وهؤلاء هم العملاء، وهذه كافة الأعمال التي نقوم بها معًا، ولدينا تنسيق كبير بينها. كذلك، ليست هناك مشكلات ولا أخطاء ولا يوجد بالقطع أي تأخير في أي تحديثات أبدًا ولا يهتم أحد ببراءات الاختراع. الشريحة التالية.

تستند العديد من الأنظمة التي يستخدمها الناس لنشر المعلومات في DNS إلى ما يسمى أنظمة التقديم. وهي ليست فقط ملفات [غير مسموع] اعتاد الناس على استخدامها القرن الماضي. فهي تمثل كافة أنواع الطرق الأخرى للقيام بهذا ومن المستحيل سرد أو اكتشاف كافة وسائل الاختراق المختلفة المستخدمة في كل مكان في العالم.

لذا، عندما يجب نشر شيء في DNS، فعادة ما يترك لكل مؤسسة أو منظمة وضع تحديثاتها على واجهاتها الخاصة وأدواتها لنشر شيء جديد. على أن هذا لا يسري على DNSsec، بل فقط على أنواع PR الجديدة والأمور الأخرى. لذا، تصبح DNS، حسنًا، سترون لاحقًا ماذا أصبحت. الشريحة التالية.

حسنًا، ذكر دان العديد من هذه الأمور، ولكن لماذا لا يستخدم الأشخاص الخوارزميات المناسبة مثل المنحنى الإهليجي؟ حسنًا، قد يكون هناك على مستوى السجل قاعدة تقول "نسمح بهذه الخوارزميات." فمن أين تأتي هذه القاعدة؟ حسنًا، إنها تتضمن هذه القائمة التي ذكرها دان سابقًا. كذلك، لا يتم الحفاظ على البرنامج الذي يقوم بهذا التسجيل أو تقديم الخدمة بعد ذلك أو نظام التوفير أو واجهة المستخدم. كذلك، ليس هناك أي مطورين.

كذلك، بخصوص HSM، لأن بعض الناس يستخدمونها، ومن ثم لا يدعم هذا الخوارزمية الجديدة لأن الجهاز قديم. كما قد تكون هناك أيضًا سياسات وطنية تحدد استخدامات الخوارزميات. حسنًا. بالإضافة إلى ذلك، تمثل إدارة توفير الموارد أحد الأمور الشائعة للغاية التي نسمعها. فلماذا ذلك؟ استغرق أحد السجلات بدون اسم سنة كاملة لدعم الخوارزمية 13، بسبب عدم وجود موارد. ولن أحدد اسمه.

بحيادية تامة، من الصعب بالفعل أن توضح للمدراء أن هناك فائدة في القيام بهذه الأمور. فسوف يسألون، "هل سيحقق هذا زيادة في الإيرادات؟" والإجابة هي "لا". "هل سيحسن هذا من صورتنا؟" "ربما." "هل سيتسبب في أخطاء." "ربما." "حسنًا. الموضوع التالي." ويعتقد الجميع أنها ليست مشكلته.

أيضًا، لدينا مشكلة النشر المثيرة بشأن قياس التشفير الجديد. وبافتراض عدم مشاركة الأصول، وأن علينا فقط التعامل مع المجتمع الأكاديمي، فعلينا الموافقة على أن تكنولوجيا التشفير الرائعة الجديدة لا بأس بها. وأنا أقدم لهذا عشر سنوات، وربما سبع سنوات. كذلك، سيكون هناك بعض المتحمسين الذين يريدون القفز على العربة مبكرًا، أو ربما يكون هناك بعض الآخرين الذين يريدون القيام بذلك لاحقًا. حسنًا.

لذا، ربما سيتم تحديد الخوارزمية الجديدة، وسيكون هناك عشر سنوات حتى توحيدها في معايير فريق عمل هندسة الإنترنت. ويمكن أن تعرض في مكاتب البرامج في مختلف الأوقات، وهذا مستقل تمامًا.

كذلك، تعتمد DNSsec ذلك في وقت لاحق كما يفعل فريق عمل هندسة الإنترنت، وقد يكون هذا شهرًا أو نفس الوقت، أو بضعة سنوات لاحقة. الآن، نصل إلى دورة الإصدار. ولا يمكن لأي شخص إصدار برنامج يدعم هذا حتى يحب الأطفال الرقم 13 أو 14 أو 15 أو مهما يكن الرقم الجديد. ومن باب التفاؤل، بالنسبة للبرامج الرئيسية، ننظر في دورة الإصدار، من موردي OS لأكثر من 10 سنوات.

وإذا تحدثنا عن برامج المؤسسة، فربما ننظر في ست سنوات. كما أني لا أزال أرى برامج ثنائية مفتوحة على الشبكة والتي تستخدم Red Hat 3. تم إصدار هذا تقريبًا كل قرن، تقريبًا. حسنًا. بعد ذلك، تكون دورة الإصدار على مستوى هذه المؤسسات بالكامل،

والبرامج على مستوى المنظمة. حسنًا [غير مسموع]، لا يوجد. وعند الانتهاء عندما يدفع شخص ما بما يكفي من القوة والطول، ويدفع الناس دفعًا للتقديم. الشريحة التالية.

لذا، إذا كان علينا الإضافة إلى الخوارزمية الجديدة، فالأمر يتعلق ككل بالمدافعين عن القيام بهذه المهمة، وتشجيع بقية العالم على التواجد. كما يصعب بالفعل القيام بهذه الأمور. ولا يمكننا افتراض معرفة الناس بما يفعلون، فقط مثلما قال [غير مسموع]. كذلك، لدينا شركات الاتصالات التي تقوم بنفس التغليف. فهل يعرفون ما يجري هناك؟ هل يعرفون أن التحقق من DNSsec يجري هناك؟ ليست لدينا أدنى فكرة.

وكذلك، سيكون هناك الكثير من الأشخاص الذين يقولون أن هذا لن يحدث قط، ولن ينجح قط. لكنه سيكون كذلك. الشريحة التالية. لذا، يمكننا جذب انتباه الناس مرة كل فترة. ولا يمكننا القيام بهذا طوال الوقت. لذا، يبج أن يكون لدينا سبب جيد لطرح خوارزمية جديدة. ويعتبر الانتقال إلى توقيعات أصغر بكثير سببًا جيدًا. ويعتبر الانتقال إلى خوارزمية أقوى بكثير سببًا جيدًا. كما يعتبر الانتقال إلى خوارزمية أسرع بنفس خصائص الأمن أو خصائص أفضل من المستخدمة الآن سببًا جيدًا. لذا، علينا تقدير السبب.

الأهم من ذلك، أن علينا تعليم الناس الموجودين في قطاع DNS أو يشعلون DNS أن ذلك ليس الوضع الراهن. فالأمور ستتغير مرة كل فترة. وحتى يمكننا الحصول على متخصصي التشفير لابتكار خوارزميات لا يمكن أن تتعطل، فسنكون في هذه المساحة. كذلك، في حالة ابتكار أحد لأجهزة كمبيوتر للحوسبة الكمية، فسأتقاعد. الشريحة التالية.

لذا، يجب أن يكون هناك سبب جيد كما قلت، لذان علينا ألا نتوقف عند الخوارزميات، فقط لأن شخص ما يعتقد أنها أفضل من تلك لدى أوندريج أو DJB أو مهما يكن. وعلينا التحقق من تكاليف ذلك، وعلينا استبعاد القديمة، كما سيكون من اللطيف بالفعل أن تستبعد جوجل خيار وجود رقم خوارزمية غير محدد مستبعد من واجهة المستخدم.

كما أننا نحتاج لقياس أحسن مما يقوم به جيوف، ونحتاج للتمكن من عرض هذه الأمور التي تعمل بالفعل. لكن هذا سيكون بطيئًا. ولذلك، فنحن نعمل جميعًا كجيمس [غير مسموع].

دان يورك: هل تلك هي النقطة المقصودة؟ حسنًا. حسنًا، شكرًا لك، أولافور. حسنًا، لذا، الآن، سمعنا من أولافور عن سبب أن هذه الأمر ستستغرق العمر كله، وستكون بطيئة للغاية كما أنها قد لا تحدث كثيرًا. وبهذا، سننتقل إلى أندريج ليخبرنا عن سبب حدوث هذا.

أولافور جوموندسون: لا أعتقد أننا مختلفون [غير مسموع].

دان يورك: أوه، حسنًا. أردت الجدال فحسب.

أوندريج سوري: لن يكون هناك صراع.

دان يورك: هيا.

أوندريج سوري: أنا أوندريج سوري من cz.nic ولدي أيضًا مسودتان في أعمال فريق عمل هندسة الإنترنت للمنحنيات الجديدة في DNSsec. الشريحة التالية من فضلك.

عذرًا، على الحروف الصغيرة. لكني لا أراها بنفسي. على أي حال، هذا عمل دانيال بيرمشتاين، غير الشهير في مجتمع DNS لأنه أحد الأشخاص المحظورين من مقدمي الأسماء. لكن هذا نوع من الانتقام له لطرح خوارزميته في DNSsec. لذا، المنحنيات الآمنة، إن لم أكن أعرف، لقد عملت معه وتيجاني لانج من الجامعة الألمانية، وقد أوضحا بالأساس وجود اختلاف بين الخصائص النظرية والعملية لخوارزمية المنحنى. كما أنها قد تختلف.

لذا، فقد حددوا مجموعة أخرى من المتطلبات لخوارزمية المنحنى الإهليجي حتى تكون آمنة. وإذا كنتم مهتمين أكثر بذلك، فعليكم النظر في الصفحة. فأنا لست باحثًا أمنيًا، بل مجرد مفكر أمني. فقط لتوصيل القطع معًا. الشريحة التالية، من فضلك.

لذا، هذه مجموعة أخرى من خوارزميات المنحنى الإهليجي. وهي منحنى إدوارد الذي يتضمن خصائص مختلفة عن ECDSA. لذا، لدى EdDSA أداء مرتفع، ولكنه ليس مثل العمل في Go وCloudFlare لصالح ECDSA، إلا أنه لا يزال أفضل من خوارزميات ECDSA. لذا، لا يتطلب الأمر ترقيم فريد لكل توقيع، وهو الأمر الجيد. فهو الأكثر مرونة بالنسبة لهجمات القنوات الجانبية. كما لنه يتضمن مفاتيح عامة صغيرة للتي سأحددها في DNSsec.

كذلك، تعتبر المعادلات موحدة تمامًا، لذا، فهي سارية لكافة النقاط على المنحنى، ولذا، لا توجد استثناءات، لأن الاستثناءات قد تكشف عن بعض المعلومات حول المفتاح الخاص. والخوارزمية تكون مقاومة للصدمات كذلك. الشريحة التالية من فضلك.

لذا، هذان منحنيان غير معتمدان من مجموعة أبحاث منتدى التشفير في فريق عمل هندسة الإنترنت. وهما المنحنيان أرقام 25519 و448، بما يسمى كذلك جولديلوكس. وقد حدد الأول دانيال برنشتاين في 2006، لذا، كانت السنوات من العرض الذي قدمته. لذا، بعدها بعشر سنوات، تم اعتماده من فريق عمل هندسة الإنترنت، لذا، فأنتم جيدون، ونحن على المسار. وقد كانت تتضمن هدفًا أمنيًا 128 بت، وهو الأمر الذي يصل بالكاد إلى [غير مسموع] 3 آلاف.

كذلك، كان المنحنى الثاني أسرع لأنه تم تحديده في 2014 من قبل مايك هامبورج، وهو حتى أقوى. لذا، فهو يقارن بـ RSA بقيمة 15 ألف، أو شئ من هذا القبيل، رقم مرتفع بالفعل. الشريحة التالية من فضلك.

لذا، هناك اثنان من المسودات لـ DNSsec، لمفاتيح DNS ولكليهما. حسنًا، قدمت بالفعل الثانية لكم، [غير مسموع] مجموعة العمل، أمس، لذا، فهذه الشراءح لم يتم تحديثها. لذا، لقد تم اعتماد كليهما في مجموعة عمل CURDLE ولأول واحدة في ed25519،

هناك إجماع على استخدام DNSsec، وأعتقد أنه مكتمل تقريبًا، لذا، رجاءً، إن كان لديكم وقت فالرجاء مراجعة الوثيقة.

كما أن الموضوع معلق بالأساس بانتظار الصياغة باستخدام [غير مسموع] المستخدمين ومسودة IETF EDDSA. وقد تم تقديم المسودة الثانية أمس. كذلك، هناك بعض المنافسين، حسنًا يوجد منافس واحد، باول هوفمان، لذا، إن كنتم تشعرون بصورة أو بأخرى باستخدام ed448 في DNSsec، فرجاء القدوم إلى مجموعة عمل CURDLE وقول ذلك، بحيث نعرف ما نقوم به، ولكن هناك خيارات محتملة لاستبعاد هذا.

حسنًا، مع وجود هذا [غير مسموع] المستقل أو مجرد دمجها معًا. ولا أهتم بالفعل بطريقة أو بأخرى، ولكننا نحتاج لاتخاذ قرار في نهاية المطاف. كما يجب أن تكون هناك ربما مسودة مستقبلية [غير مسموع] ذكر أيضًا شيئًا يخص التخلص من الخوارزمية القديمة التي يجب عدم استخدامها بعد ذلك مثل DSA على سبيل المثال. الشريحة التالية من فضلك.

لذا، أعتقد أنه تم ذكر معظم الموضوع بالفعل، لذا، سأقول فقط أننا سيكون لدينا ورشة عمل مماثلة في DNS-OARC، في بيونس آيريس، لكننا سندعو موردي DNS، أيضًا. كما سنتابع الحديث هناك. لذا، نرحب بكم جميعًا، للقدوم والمشاركة. وحسنًا، أعتقد أننا متفقين بالأساس من قبل أن هذا سيستغرق الكثير من الوقت، لذا، فهدفي أنه عندما نطرح المفاتيح خلال عشر سنوات، فإن مفتاح الخادم الجذر، يمكننا ربما استخدام هذا كخوارزمية. حسنًا، اعتقد أن العشر سنوات هو هدف متفائل. شكرًا.

دان يورك: شكرًا لك، أندريج. ونعم، يمكن أن يقدر روس الدفع نحو اللجنة القادمة. كما سنتحدث عن مفتاح الدخول الرئيسي بقدر ما سيكون الإطار الزمني بالفعل. هل سيكون 2026؟ وهل سمعناه هنا الآن؟ لذا، أود فتح الباب للأسئلة وسأطرح سؤالاً واحدًا فحسب لأندريج، عندما يقول أن ورشة العمل ستكون DNS-OARC، هل يمكنك الحديث قليلاً عن هذا؟ ما الذي نحاول القيام به؟

أوندريج سوري: حسنًا، سأقول أنها كانت فكرتي وأنا أدعو الناس تقريبًا من موردي DNS وأنظمة التشغيل مثل العاملين في Red Hat، وRed Hat 3، وعلينا الحديث أكثر عن دورات الحياة للبرامج، ودورة حياة النشر، أود متابعة النقاش. ما الذي يمكننا أن نفعله لتسريع ذلك؟ لأن الأشخاص [غير مسموع] يمكنهم القيام بهذا، بالأساس، وهناك شيء خطأ في DNS بأننا لا يمكننا القيام بهذا.

لذا، أعتقد أن هذا وقت تغير الأسلوب، والذي كنا نعمل عليه، وسيصعب تغيير الأسلوب، كأي تغيير مماثل. مع ذلك، يلزم القيم بهذا، ونحتاج لمزيد من المرونة من جانب الخوارزميات في DNSsec حتى نجعل الأمور ناجحة في المستقبل، وهذا بالفعل [غير مسموع] من تحديد الخوارزمية إلى النشر وقت طويل بالفعل، ويلزم تقصير هذا الوقت قصيرًا.

بول هوفمان: لذا، يمكنني الرد على هذا. فجزء من المشكلة غير متعلق تماما بكل هذا. وهي تتعلق بشهادات FIPS والعملية في NIST. لذا، تدرك NIST هذا وهناك برنامج بدأ مؤخرًا لتكرار العملية بالكامل لشهادات FIPS. لذا، بهذا، سنتمكن من تسريع العملية في حالة السماح بشحن الخوارزميات في ROS وإرسال هذه التحديثات.

كما أن NIST نفسها تخطط لهذه الطريقة المقابلة للاعتماد بحيث تكون جاهزة خلال سنتين.

دان يورك: إذن، بول. لذا، ما تقولون هنا هو أن NIST تمثل العامل الرئيسي في إدراج البرامج في [غير مسموع]؟

بول هوفمان: حسنًا، هناك اثنان. هناك اثنان. شهادة FIPS هي الأهم لأننا نرسل تحديثات منتظمة حول أنظمة التشغيل وندعمها لفترة طويلة. لذا، لا تشكل تحديثات الخوارزمية الجديدة مشكلة بالفعل لنا. كما أن FIPS تعتبر مهمة للغاية.

وقد نسيت الآن الأخرى. سأتذكر في نقطة ما.

دان يورك: حسنًا. حسنًا، أعتقد، وأوندريج، جزء من إجابتك، أيضًا، أليس كذلك؟ كما يمكن أن يكرر ذلك بائعي برامج التصفح هذا أسرع لأنهم يمكنهم وضع علامات تحذير كبيرة تقول "سيتقادم المستعرض الخاص بكم إذا لم تحدثوه الآن." ونوع هذه الأمور، كما يمكنهم القيام بهذا وسيستجيب المستخدمون. لكن لدينا طريقة أصعب للقيام بهذا مع DNS.

أوندريج سوري: لذا، عليك تذكر الأخرى. والأخرى هي ما يهتم به المحامون بالفعل، للأسف. وإذا كنتم شركة كبيرة، فعادة ما سينظر المحامون في هل يمكننا المقاضاة أم لا وما مقدار المال المتكبد؟

دان يورك: وارين، لقد نظرت لي بصورة مضحكة عندما قلت ذلك. وارين من جوجل.

وارن كوماري: وارين كوماري من جوجل. اعتقدت أنك ستقترح وضع رسائل نصية تقول، "تقادمت الخوارزمية. وعليكم طرحها قريبًا في القسم الإضافي التالي لكافة السجلات."

دان يورك: هل يمكننا القيام بذلك؟

وارن كوماري: يمكننا ذلك بالفعل.

دان يورك: نعم. هيا. وقائمة الانتظار مفتوحة.

شخص غير محدد: حسنًا. لذا، موضوع مختلف، أردت فحسب، إن كان لا بأس بهذا. حسنًا. أريد أن أرد على شيء ما قاله أولافور وأكرر ربما [غير مسموع] سبب أنه سيكون هنا، فأنا لا أعرف وسنرى. أعتقد أن أولافور وأنا على الأقل متفقين في هذا بصورة شخصية، ولكن الموضوع هنا هو التأكيد فحسب لأني أعرف أن ورشة العمل هذه وهذه الجهة لديها أفضلية بالتركيز على المشكلات الفنية. لكن ما يحدث في منطقة ICANN ومن المهم تكرار هذا، هو أننا قلنا هنا من قبل في ورشة العمل والاجتماعات السابقة وكما قال أولافور أنه هنا في النهاية، وأريد فقط أن أضايقه وأؤكد على ذلك وأتحدث قليلاً عن الأمر.

كذلك، فالأمر أن هناك بالفعل مشكلة أساسية هنا من حيث الدعم لأي شيء بشأن DNSsec. وهذه هي الحقيقة أن مزودي خدمات DNS لا يتم الاعتراف بهم كجهة مستقلة في المنظومة على الأقل ليس في مجال ICANN.

كذلك، من السهل بالنسبة لي كمزود خدمات سجل أن أقول، "حسنًا، نحن الأخبار الجيدة. ولن أعترض طريقكم بقدر ما ترتبط المؤسسة." كما أن معظم السجلات ربما لن تقوم بهذا، حتى. كذلك، قد يكون هناك البعض الذين، لأي أسباب قانونية، يدعمون تعليق المحامي السابق.

ولكن حتى إن أمكن رؤيتنا كجزء من المشكلة إلى الحد الذي توجد به أمور يحتاجها مزودي خدمات DNS ويريدون ألا نقدمها ببساطة. وما أعنيه، أن السياسات في مجال ICANN لا تسمح ببساطة بهذا، ومن المهم تذكر هذا، وهي قوة محركة في بعض المتطلبات والقدرة على نشر هذه الأمور بصورة مستقلة عن المشكلات الفنية الجارية.

لذا، شكرًا لك أولافور على إثارة هذا مرة أخرى. وأردت فحسب تكراره. كما يمكنكم النظر هنا من خلال ورش العمل السابقة. كما ترون، فقد غطينا هذه المشكلة بالتحديد بالتفصيل في أماكن أخرى وسنرى ما إن كان أولافور يريد الإضافة إلى ذلك. شكرًا.

دان يورك: على ما يبدو لا. حسنًا. لذا، فهو صراع من جانب واحد، ولكن جيوف، يمكن أن تكون استباقيًا. ها نحن أولاء.

جيوف هوستن: أنت على حق. يتمثل جزء من هذه المشكلة، خاصة، بشأن تشفير المنحنى الإهليجي، والسؤال الفعلي هو لماذا يجلس واحد من بين ستة من المستخدمين وراء المحللين الذين لا يقبلون هذا التشفير؟ الآن، تتمثل المراقبة في عامل التشفير، وهناك قدر كبير من الثقافات الأحادية الموجودة. وبالفعل يوجد قدر هائل من البرامج التي تستخدم مكتبة OpenSSL.

الآن، كان الأمر حول تشفير المنحنى الإهليجي أنه لفترة زمنية حتى أعتقد أنه كان في أول الألفية الجديدة، ربما منتصف العقد الأول منها، في مكان ما، كان هناك نزاع حول حقوق الملكية الفكرية لشركة تسمى Certicom حول من يمتلك تشفير المنحنى الإهليجي.

وقد دفعت الشكوك حول حقوق الملكية الفكرية عددًا من الموزعين للبرامج إلى ترك تشفير المنحنى الإهليجي خارج الحزمة التي يقدموها. وبهذا، فما كان يجري في العالم في هذا الوقت ربما كانت Red Hat 3، ولا أعرف بالفعل، ولكن شخص ما سيعرف، أن هذه الإصدارات الأولى لم تتضمن دعمًا للمنحنى الإهليجي.

كما أنها الآن موجودة في OpenSSL لأكثر من عشر سنوات الآن. ونفهم أنه في حالة وجود حزمة الآن، فستتضمن تشفير المنحنى الإهليجي. لذا، فلما يجلس واحد من بين ستة مستخدمين وراء الأمور بدون تفكير التي لا يفهمونها؟

يرجع ذلك إلى أن ما هو موجود قد يكون قديمًا للغاية في بعض الحالات. كما أن هذه المجموعة من الشك في حقوق استخدام بعض الملكية الفكرية، التي تشكل مشكلة لنا جميعًا بالفعل، مع الدوائر البطيئة للغاية بالفعل، حتى بعد المرور بكافة المعايير، فإن الدوائر الطويلة للغاية لما يقوم به الزملاء مع محللي DNS.

كما أنه من المؤكد في بيئة العمليات انه بالنسبة للعديد من مشغلي ISP، فإن تشغيل المحلل يحدث مرة في العمر. وبعد ذلك، عليهم فقط تركه وحده. لذا، ما يحدث هو أنه مهما تكن نقاط الضعف في ذلك الوقت، فيجب البقاء هناك.

دان يورك: يمكننا طرح سؤال هنا. لذا، كم عدد الأشخاص في الموجه المنزلي أو موجه واي فاي منزلي في، ليس كذلك. وما نسميه موجه، أليس كذلك؟ ولكنه ليس كذلك، أعرف بالنسبة للجمهور هو أحد هذه الأمور، أليس كذلك؟ كما أننا نحصل جميعًا على صناديق صغيرة، أليس كذلك؟ وفي نهاية الشبكة. حسنًا. من بين هؤلاء الناس الذين يرفعون أيديهم، كم عدد الأشخاص الذين حدثوا البرنامج في أي وقت مؤخرًا؟ أوه، انظروا إلى هذا. نحن حشد عبقري بالفعل.

حسنًا، مؤخرًا. حسنًا. خلال آخر عام.

شخص غير محدد: هل يشكل فارقًا شراء واحد جديد؟

دان يورك: شراء واحد جديد، حسنًا. حسنًا. دعوني أوجه لكم سؤالًا. ربما لدى كل منكم عائلة آمنة، حسنًا، من لديه هذه في منزله. وما عدد المرات التي ترون أن عائلتهم تحدث البرامج بها مؤخرًا؟ حسنًا. حسنًا، نعم. حسنًا. تقدمون لهم كافة صناديق السياح، أليس كذلك؟ حسنًا. أجل. بالنسبة للوافدين الجدد، هؤلاء هم الزملاء من cz.nic الذين لديهم صندوق صغير لطيف يدار ككل ولذا، يدفعون التحديثات تلقائيًا وأمور مثل هذا. لذا، بالطبع سيقومون بإطلاق الجميع على التحديثات.

وبالنسبة للأشخاص خارج جمهورية التشيك، أو خارج أوروبا، لا بأس؟ من ليس لديه صناديق خارجية، للجميع أيضًا. ربما أنا في الحشد الخاطئ لطرح هذا السؤال. أسئلة أخرى. لقد رأيت شخصًا ما. روبرت. وبعدها، رأيت داني وشخص آخر؟ حسنًا.

روبرت مارتن ليجين: حسنًا. أنا مواطن مجهول. إذا كان لديكم أي تثبيت قديم لخادم لم تحدثوه منذ أربع سنوات، ربما لا تستحقون التحقق من أنه يعمل في حالة تشغيل ECC.

دان يورك: لا يستحق جمهور المستخدمين الجاهل الأمن الإضافة وهذا ما نقوله. لا أعتقد أن هذا مفيد، روبرت. حسنًا. حسنًا، داني.

روبرت مارتن ليجين: حسنًا، أنا مخفي.

دان يورك: عذرًا. أياً كانت هويتك. هل تريد الرد؟

شخص غير محدد: أردت فقط الرد على تعليق جيوف بأنه لا توجد نزاعات ملكية فكرية على خوارزميات ED محددة في المسودات.

شخص غير محدد: انتهت براءات الاختراع في 2012 و13 و14.

شخص غير محدد: ها نحن ذا. يعرف الأشخاص الكثير عن ذلك عني، ولكني سمعت أيضًا أنه لا توجد نزاعات متبقية على استخدام هذا واليوم هناك بعيدًا عن وارين هناك استخدام [غير مسموع] لذلك.

شخص غير محدد: كما أنا لا يمكنني حتى الحديث عنها عبر البريد الإلكتروني مع المحامين.

دان يورك: حسنًا، داني.

داني جرانت: من جانب أمين السجل والسجل، ما السبب في القيام بأي تحقق حول رقم الخوارزمية؟

دان يورك: حسنًا. حرب دينية مفتوحة.

شخص غير محدد: لقد قدمتم للناس قائمة وتحققتم من صحتها.

دان يورك: أي شخص. وارين هل تريد؟ حسنًا. أرى أن وارن يرغب في المشاركة.

وارن كوماري: لذا، يرجع هذا إلى أن المستخدمين ليسوا دائمًا الأسرع، ولذا، أعني أن جوجل العام أو لأمناء السجل تتضمن أمرًا من واحد أو ثلاثة وما إلى ذلك الارقام بجانبها. ومن الصعب للغاية فقط أن نجعل المستخدمين يفهمون ما تعنيه هذه الأرقام. أعرف أن هناك من الأشخاص من قال "حسنًا، من الرائع أنكم أضفتم الأرقام." وبعض المستخدمين ليس لديهم أدنى فكرة عما هو الأمر، وعندما نرى 13، ECDSA، فهم يحاولون لصق مفتاح ECDSA 13 مرة وبعدها صابون بالإحباط.

أو يعتقدون أنهم يحتاجون 13 نسخة منه. والأمر يصعب على الأشخاص بالفعل فهمه. كذلك، هذا النوع من الأمور المعروضة في الصناديق، هناك التحقق، ولكن توجد لديهم أمور مثل نعم، رجاءً، أود، على المدى الطويل بالطريقة التي سيكون لديك DS، ضعه في DS.

لذا، للأسف، تحتاجون للقيام ببعض الفحص الصحي، وأعتقد أنه موضوع مطروح بشكل ما.

داني جرانت: من وجهة نظري، هذه مشكلة قابلة للحل، أليس كذلك؟ لذا، يمنكم قول، في UI، هناك مجموعة محدودة من الخيارات، ولكنه إذا كنتم تستخدمون API، فلديكم حرية استخدام مهما يكن. لذا، بالفعل، لا يزال السؤال قائمًا. وأنتم تقولون، "لماذا يجب أن يكون هناك تحقق على الإطلاق؟"

دان يورك: جيم. وأعرف أنكم تريدون المشاركة.

جيم غالفين: لذا، حسنًا، علينا فصل بضعة مشكلات هنا، وأعتقد أنكم مستفزون فحسب هنا. كذلك، هناك، من بين هذه المجموعة الكاملة من مشكلات واجهات المستخدم والتعامل مع المستخدم، وهناك مختلف طرق التعامل مع هذه المشكلة. من جانب السجل، سأوجههم إلى هذا بالنسبة لنا، وليس لدينا أي قيود محددة على ما تقومون به، لذا، سنترككم تقومون بأي شيء طالما هي خوارزمية مدرجة صحيحة وفق المعايير التقنية.

داني جرانت: وهذا ما أسأل عنه. لماذا نحتاج للتحقق من هذا؟

جيم غالفين: كما تعرف، أنت محق. من وجهة نظرة عملية، ليس على المرء بالفعل القيام بهذا، ولكن نحاول احترام المعايير. لذا، من وجهة نظرنا، عليكم عدم السماح بالقيام بشيء ما، لا يكون معترفًا به في الدولة كأمر يمكن القيام به، وكما تعرفون، أعني أننا لا نترككم تقومون بأمور حمقاء، هل علينا قول هذا؟ فنحن نبذل قصارى جهدنا لمنع ذلك. حسناً؟

لذلك، فأحد الأمور التي نريدها هي فحص هذا النوع من الأمور. ويمكن أن يكون لدينا بالتأكيد حول ما إذا كان هذا عادلاً للقيام به أم لا على هذا المستوى. حسناً؟ على الرغم من ذلك، يتمثل الجانب من ذلك في أنه في بعض الأحيان، إذا كنتم سجلاً، وأخذتم المفتاح وتقومون بإنشاء سجل DS نيابة عن المستخدم، فقد تكون هناك قيود على ما يمكنكم القيام به هناك. حسنًا؟

ولهذا السبب، ربما توجد قيود على الخوارزميات المسموح لكم باستخدامها وأخذها من المستخدم، والعلاقة القائمة وسوف تنفذون هذا. وهذا هو التقييد من هذا الجانب. وهذا أحد الأسباب بأننا لا نأخذ المفاتيح، فنحن نأخذ فقط DS، ونود أن نترك جميع هذه الأمور تمر. كما أننا نجري فحصًا صحيًا عليها لأننا نعتقد أنه مناسب.

دان يورك: كذلك، ندخل في موقف يقدم للمطورين قائمة وسيتحقق منها. ولدينا مجموعة كاملة لمطوري الويب على وجه التحديد الذين يرهقون عقولهم في أنهم يحتاجون للذهاب والقيام بهذا الفحص للأمن.

جيم غالفين: حسنًا، ولكني فقط اقول أنها عقلية، حسنًا؟ وبالرغم من القيام بهذا الفحص حول مهما يكن ما يمكنكم. لذا، إن حصلتم على القائمة، فعليكم فحصها. هذا ما تقومون به.

دان يورك: [غير مسموع].

جيم غالفين: حسنًا، الأمر الأخير الذي أود إضافته لدفع مجموعة التحقق من الأمور. الأمر الآخر للأسف، أن علينا التعامل مع هذه الأمور في وقت ما، خاصة مشغل السجل أو ربما وضع الدولة سيكون لها خيارات حول الخوارزميات المتاحة للاستخدام. حسناً؟ وآسف، أعني كمزود خدمات، علينا اعتماد هذا. ولكن علينا فقط التعايش معها ولا يمكننا الاعتراض على هذا. عذرًا.

دان يورك: لذا، أعرف أنك تريد الرد على هذا، وبعدها لدينا سؤال في الدردشة، وبعدها سنحتاج للاختصار، ولكن تفضل.

[آرون لانسينج]: 16 ثانية، نعم، سأحاول. [آرون لانسينج]، ممثل الدانمارك. أردت الرد بطريقتين الأول هي أن لدينا خدمة عملاء. لذا، لا نتيح للعملاء القيام بالفعل بأمور حمقاء لأن هذا يدفعنا فقط للحديث معهم. الأمر الآخر الذي أردت فتحه بالفعل هو الخدمة الذاتية الجديدة الصادرة مؤخرًا. وقد فتحنا الفحص العقلي بالأساس، فما عدد الأرقام الموضوعة فيه؟ من الألف إلى الياء، من واحد إلى عشرة، وهذا الرقم الصحيح مقارنة بالخوارزمية التي قامت بدور ما.

الأمر الآخر الذي أردت قوله، وأنا أريد [غير مسموع] بهذا الشأن، وقد كانت من فكرة من [غير مسموع] مع أولافور أن نضيف زر صغير في الخدمة الذاتية لدينا يقول "الحصول على سجل DS." لذا، تأتي خدمة المبيعات لدينا، عبر TCP، بالطبع، وعبر نفس خوادم الاسم الموجودة لدينا في نظام WHOIS، فلدينا السجل. ويحصل على المفتاح ويحسب سجلات DS قبل أن يقول للمستخدم "هل هذا هو سجل DS الذي تريده؟" وينقر المستخدم فوق نعم فحسب، بدون نسخ ولصق.

وهذه UI. ويرجع هذا إلى أننا سجل غريب يتحدث بالفعل إلى المشتركين وكمشغلين.

دان يورك: رائع. الآن، أرى السؤال قادم من، تفضل.

داني جرانت: إنه ليس سؤالاً، بل تعليق، ولكن التعليقات أيضًا تقرأ للسجل. إنه من [أنطوني جيرشوين]. فهو يعلق "بعض السجلات تقيد الخوارزميات لأنها تريد أن تتمكن من استبعاد الخوارزميات القديمة بمجرد أن تصبح غير آمنة، وعدم استبعاد الأحدث، فالهدف ليس تحقيق أقصى قدر ممكن من النقود من خلال تسجيل أقصى عدد ممكن من النطاقات، ولا نهتم ما إذا كانت معطلة. وهذه هي مخاوفي الخاصة.

كذلك، يمكن أن يكون لدينا هدف مختلف مثل الثقة والأمن، ونريد إدارة الصورة العامة للنطاق وليس صورة المنطقة ولكن النطاق. ولا توجد سياسة واحدة توافق كافة نطاقات TLD، فهي ليست رأسمالية أو ديمقراطية أو اشتراكية أو متعددة أصحاب المصلحة،

اختر توجهك. وبقول هذا، أعتقد أنهم يجب أن ينفذوا خوارزميات جديدة أفضل أسرع ولكن ليس هناك ما هو سيء في عدم موافقة الخوارزميات غير الآمن من قبل الأصول.

دان يورك: نقطة رائعة من [أنطوني]، إنها مناسبة. وأعني، نقطة تقييد والتخلص التدريجي من القديمة. حسنًا، بشكل سريع. روبرت وبعده داني.

روبرت مارتن ليجين: كيف تعرفون ما إذا كنت كذلك؟

دان يورك: أياً كانت هويتك. أود فقط أن [غير مسموع].

روبرت مارتن ليجين: لم أعد مجهولاً بعد الآن. روبرت من PCH. وأنا أتساءل فقط عما إذا كان أي شخص لديه أي خبرة في المنع الفعلي لبعض خوارزميات DS غير الآمنة وما سيكون الأمر، وهل سيتم حذفها وعدم تأمينها للمستهلك أم ماذا؟

دان يورك: أجل. هل من أحد؟ لا.

شخص غير محدد: سأقول فحسب أنه طالما هي على القائمة. أعني، يجب أن يستبعدها فريق عمل هندسة الإنترنت من القائمة قبل أن نتمكن من حذفها. وأعني، نشعر فحسب بالتزام بدعم المعايير في هذا الصدد. كما أننا لا نريد أن ينظر إلينا كجهة تشفير أو شرطة أمنية في العالم.

روبرت مارتن ليجين: ولكن بعد ذلك، تتركون غير المسجل بدلاً من التسجيل الضعيف.

شخص غير محدد: حسنًا. أعتقد أنه ليس [غير مسموع]، وشكرًا. كما سأقول فحسب أن ذلك جزء من الخوارزميات للتشفير، وهذه أيضًا خوارزميات للتجزئة وبالفعل نعم، عندما نحصل على هذا النوع الأول والنوع الثاني، لتنفيذ النوع الأول حيث سنحذفه وفقط استبعاده. كذلك، كان لدينا تسجيل واحد مقدم سواء النوع الثاني والنوع الثالث، وقد طرحت كليهما، كما أعتقد أنه من المناسب القيام بهذا، لم يكن هذا السؤال بالفعل الذي أود طرحه.

فهل نشعر أننا يجب أن نقوم بأنواع متعددة مفيدة؟ ولكن هذه مناقشة طويلة، ربما ليس لهذا القاعة الآن.

دان يورك: كذلك، أنتم محقون تمامًا لأن الوقت يداهمنا وأحتاج لتقديم لجنة جديدة، ولكنكم كان لديكم تعليقًا نهائيًا.

داني جرانت: لا بأس.

دان يورك: لا بأس. حسنًا. حسنًا، لا أعرف أننا قمنا بحل أي أمور هنا، ولكننا تحدثنا عن الأمر، كما أعتقد أننا تحدثنا عن ماهية التحديات. وقد كان هذا جيدًا، وسمعت بعض الأفكار الجديدة الجيدة من هذا. كما أعتقد أن ما أشجع الناس على القيام به هو النظر في المسودات التي قدمها أوندريج والموجودة هناك لأن هذا يمثل المسار المناسب عند الحاجة لطرح DNSsec أقوى في هذا الصدد.

علاوة على ما تقدم، سمعتم جميعًا عن المشكلات المطروحة هنا حول كيفية نشر هذا، وأريد أن أسمع الأفكار حول ما نقوم به، على أني أدعو الناس للتفكير في ورشة عمل ICANN DNSsec التالية، هل هناك أمور يمكن طرحها فيها، وما هي الحلول التي يمكننا وضعها لتسريع الأعمال؟

ودعونا نتحدث إلى أوندريج إن أردتم المشاركة مع ورشة العمل في DNS-OARC قبل بيونس آيريس في فريق عمل هندسة الإنترنت. وبهذا، دعوني نأخذ جولة من التصفيق لأعضاء اللجنة وسنقدم لجنة أخرى هنا.

روس موندي: هل ترك أي شخص السترة هناك؟ هل يعرف أي شخص بذلك؟ هل يريد أي أحد سترة رمادية؟

شخص غير محدد: إنها طريقة رائعة من واشنطن العاصمة، وبوضوح. الرجال بمقاس كبير للغاية، خمسة دولارات.

شخص غير محدد: مرحبًا. وقتكم يقترب من الانتهاء.

روس موندي: أتمنى أن يطالب أحد بالسترة هنا. مع استمرار مناقشات اللجنة، أناروس موندي من SSAC. وParsons هي من يوظفني. كما أننا سيكون لدينا آخر جلسة لليوم، بالحديث عن طرح مفتاح منطقة خادم الجذر من بضعة وجهات نظر. الأول، والذي سأقوله باختصار، سيرتبط بما نشرته SSAC نفسها بشأن طرح مفتاح ملف الجذر.

بعد ذلك، لدينا جيوف هيوستون يخبرنا عن نتائج فريق التصميم المشكل السنة السابقة، مع العمل لعدة شهور وتم إصدار التقرير يوم الاثنين. أجل. وأعتقد أنه كان يوم الاثنين. لذا، فقد انتهي ذلك وهو بالفعل متوفر في هذا التوقيت. بعد ذلك، سيقدم لنا وارين كوماري من جوجل بعض وجهات النظر بشأن التأثير وبعض التأثير المتوقع للمستخدم النهائي من طرح مفتاح ملف الجذر. كما أن وارين بالرغم من ذلك ليس مرتبطًا بصورة مباشرة بتشغيل محلل جوجل للتحقق من الصحة، وهو شخص ذكي ويعرف الكثير وسيخبرنا بنقاط جيدة.

شخص غير محدد: لذا، فعلينا ترك الكلمة له كما يقول الناس.

روس موندي: حسنًا. لذا، أولاً، اللجان الاستشارية في SSAC والتعليقات على طرح مفتاح الخادم الجذر. الشريحة التالية، من فضلك. يوجد بالفعل اثنان مرتبطان بها. الأولى هي SAC 63، ويسمى الاستشارات حول طرح مفتاح DNSsec في منطقة الجذر. نعم التالية.

علاوة على ما تقدم، كانت هناك سلسلة من المناقشات داخل SSAC لحوالي سنة ونصف. لذا، رأت SSAC أن هذا موضوع مهم للغاية لعدد من السنوات وأردنا أن نشجع المجتمع على بدء اتخاذ الخطوات قبل فترة طويلة قبل فترة خمس سنوات تقريبًا عندما كان يقصد من مفتاح الجذر هو الطرح قبل ذلك وبعد على الأقل إغلاق الإطار الزمني. لذا، فهذا هو سبب أننا بدأنا العمل على هذا بالفعل في 2012، وقد تم نشره في 2013.

لذا، في الوثيقة نفسها، تقدم بضعة مجالات من النص المسرود يتحدث عن الخلفية وما عرضته SSAC كأمور مهمة للتفكير فيها ومراعاته كجزء من عملية الطرح. والسبب في أني ذكرت أن هذا الإطار الزمني يكون مع مرور الوقت ضمن الساعة الزمنية الفعلية، أن بعض الأمور المهمة والتي يمكن أن يكون لها تأثير كبير ستتغير.

وبهذا، من الوثيقة أو الأوصاف التي سنسمعها في اللجنة، فهذه أقدم وثيقة منشورة في نوفمبر 2013. لذا، يمكنكم رؤية مواطن الموضوعات العامة وسأنتقل فحسب إلى التوصيات التالية.

لذا، فقد تمت الإشارات إلى التوصية الأولى بصورة كبيرة في فريق عمل ICANN وكذلك شركاء إدارة ملف خادم الجذر، الذين يمثلون الحد الأدنى. ولا يزال ساريًا أن NTIA ووزارة التجارة الأمريكية، وVerisign بجانب ICANN. لذلك، فهذه ثلاثة أطراف تحتاج للمشاركة بشدة في حملة الاتصالات عبر العالم للتأكد من أن العالم يعرف أن هذا سيحدث. وهذا قادم أيها الزملاء، والاستعداد لمهما يكن ما تحتاجون للقيام به، التالي، رجاءً.

ومرة أخرى، يجب أن يقود فريق عمل ICANN ويشجع وتعزيز تطوير الاختبار وأسرة الاختبار لفحص تأثيرات اطرح في الصناديق الوسطى على وجه التحديد أو الأجهزة الأخرى التي قد تتأثر بهذا بشدة. كذلك، فهذا هو التاريخ الفعلي لأحجام الردود في DNS الكبيرة بما يكفي لأن تميل بعض الأجهزة، خاصة من نوع الصندوق الأوسط، إلى السقوط، أو على الأقل أن تتعطل بدلاً من أن تظهر هذه الأمور. يرحمك الله.

لذا، تمثل التوصية الثالثة احتياجات فريق عمل ICANN للعمل عن قرب مع المجتمع لمعرفة كيفية وصف الانقطاع وكيفية وصف ذلك. ولذا، هذه بالتأكيد مخاوف من جانب SSAC بأن تكون هناك بعض المشكلات أو طبيعة ما بسبب الطرح. ولم نحاول تحديد ما هي. فقد شعرنا أن الأنسب كان سؤال فريق عمل ICANN والمجتمع لوضع ماهي بصورة عامة.

ولكن، هذا شيء مهم النظر فيه، وبهذه الطريقة، إذا كان لديكم أكثر مما تتوقعون، ومهما يكن الأمر، يمكنكم اتخاذ بعض الإجراءات. الشريحة التالية، من فضلك.

بعد ذلك، التالي، وهو يتعلق بالفعل بالأخيرة. في حالة ما إذا مضت كافة الأمور بصورة مروعة للغاية. فماذا يعنيه خاطئ أو ما مقدار التعطل الموجود؟ وعليكم الاستعداد للعودة إلى الوضع السابق. هل تحتاج للتحديد مقدمًا لمن يتخذ هذه القرارات، وماذا ستكون المعايير العامة التي تستخدمها لاتخاذ هذه القرارات.

يرجع ذلك في هذه النقطة، إلا أنه لا أحد وضع بالفعل أي شيء باستثناء طرح مفتاح التقدم. وعادة، هذا كافة ما لديكم مخاوف بالتحديد حوله، لأننا لم نقم يومًا بطرح مفتاح في حد ذاته، ولذا يوجد احتمال، أن يكون عليكم طرحه مرة أخرى، لذا، يلزم تفعيل كافة الهياكل مقدمًا والتخطيط للتعامل مع هذا.

بعد ذلك، التوصية الأخيرة هي أنكم تحتاجون لتجميع أقصى قدر ممكن من المعلومات، وهذا يتضمن أيضًا معرفة المعلومات الحساسة لتجميعها فيما يتعلق بهذا الاستبدال القادم بحيث سيكون لديكم على الأقل أساس للبيانات والمعلومات لاستخدامها في المقارنة عند حدوث الاستبدال التالي. بعبارة أخرى، تحتاجون لتجميع ما يلزم لمساعدتكم في التعلم والقيام به بصورة أفضل المرة القادمة.

لذا، فهذه هي التوصيات الخمس من SSAC. إذن، هل يمكننا الانتقال إلى الشريحة التالية، رجاءً. وبعد ذلك، في تقرير SSAC رقم 73، قدمنا تعليقات حول المسودة الأولى لإطار عمل المراجعة العامة من تقرير فريق التصميم، وهو ما سيتحدث عنه جيوف قريبًا. الشريحة التالية، من فضلك.

وهنا، ذكرنا أن مسودة فريق التصميم في هذا الصدد لم تتضمن بالفعل الكثير من المعلومات أو أي شيء بخصوص SAC 63، لذا، لديكم هنا مجموعة تعمل على التصميم الفني لاستبدال مفتاح الجذر، ولديكم مجموعة أخرى في SSAC، ICANN، والتي قالت بالفعل عددًا من الأمور حول استبدال مفتاح الجذر، ولم يصدر عنها أي تصحيح. ولذا، لاحظنا ذلك، واقترحنا أنه سيكون من الجيد أن ننظر في محاولة إدراج هذه الأمور وكذلك أن نطلب من مجلس الإدارة مرة أخرى أن يقدم المستجدات بشأن الحالة وما يحدث في SAC 63.

لذا، يمكنكم أن تروا أن هناك مجموعة أمور جارية تنظر في SSAC. بعد ذلك، لدي كاثي، تفضلي. وسنتعرض هنا للشرائح الموجودة هناك. كما أريد التقدم فحسب، والمرور بسرعة بحيث يمكننا الحفاظ على الوقت. إذن التالي.

وأنتهي بأننا سننتظر حتى نهاية عروض اللجنة وبعدها نتلقى أسئلة على هذه النقطة، لذا، رجاءً كتابتها وبعدها أنتقل إلى جيوف.

جيوف هوستن: شكرًا لك، روس. لذا، سأنتقل بسرعة عبر هذا الموضوع. نعم التالية. هذه مهمة لأننا بصراحة وصلنا الآن إلى نقطة لن يحل فيها واحد من بين ستة مستخدمين اسمًا مسجلاً بصورة غير مناسبة في DNSsec. لذا، فهذا يعني في العادة، إذا وضعتم التوقيع في DNSsec، فواحد من بين ستة لن يراكم بعدها.

لكن إن حددنا أصل التحقق، فهذا عدد الزملاء الذين سيتأثرون. نعم التالية. لذلك، هناك هذا الأمر الذي حصل في النهاية على هذا القدر الرهيب من الزخم فيما يتعلق باستخدام DNSsec لتوضيح هذا إذا تم تسجيله بصورة غير مناسبة، على أن قدر كبير من الزملاء على الإنترنت لن يمكنه أن يحل هذا الاسم، وهو ما أردناه على وجه التحديد. نعم التالية.

لذا، فهذا عدد مهم لأنه كذلك، وإذا كنتم سوف [غير مسموع] الزملاء بحيث إن حصلنا على خطأ في طرح المفتاح ودفع هؤلاء المحللين للتحقق من الصحة، حتى ستكون المشكلة في DNS في هذا اليوم. سيكون ذلك أمرًا سيئًا. نعم التالية.

لذا، نعود إلى السنوات الخمس والتسعة شهور. وقد كانت هذه تغطية في الإعلام بسبب تسجيل الأمور بالأساس في 1 يونيو من عام 2010. نعم التالية.

وهذه وثيقة مهمة للغاية. فهي بالفعل شهادة لبيان ممارسات DNSsec والتي نشرتها ICANN حول ما سيفعلون بهذا المفتاح. والآن، فهذا بيان مهم لأنه بدون بيان ممارسات، سيكون المفتاح العام مجموعة من وحدات البت فحسب. وإذا كان بيان الممارسات يقول "سنأخذ المفتاح الخاص ونكتبه ونضعه على حائط كل باب يمكننا العثور عليه"، فربما لا نثق بذلك.

والسبب الوحيد في أنكم يجب عليكم الثقة في هذا المفتاح هو هذه الوثيقة. لأن هذه الوثيقة هي التزام من ICANN نحو الطريقة التي ستدير بها مجموعة وحدات البت هذه. وعليكم فقط الثقة بهذه المجموعة، في حالة وفاء ICANN بالتزامها. كما تم تلخيص الالتزام أو مجموعة الالتزامات التي قدمتها ICANN نفسها، لم يتم فرضها عليها. وفي الواقع، فهي مذكورة في بيان الممارسات. وهي وثيقة مهمة.

كذلك، أحد أجزاء هذا محددة بدائرة هنا، وهي تقول بالأساس "سيتم طرح هذا." وهذا ما قرأته. اسمحي لي بشيء أقرب. أحتاج نظارات أفضل. سيتم تحديد كل مفتاح تسجيل رئيسي KSK لمنطقة الجذر لتغييره عبر مراسم المفتاح كما هو مطلوب، أو بعد خمس سنوات من التشغيل. نعم التالية.

لذا، عذرًا، مرة أخرى. اعتقدت أنه كانت هناك شريحة أخرى. وبعد خمس سنوات يعني العديد من الأمور للعديد من الأشخاص. كذلك، بالتأكيد من موقعنا في فريق التصميم، فقد شعرنا بالفعل بالقرب بدرجة معقولة من السنوية الخامسة لإنشاء المفتاح. بعد خمس سنوات، 2015.

وبحلول وقت التأسيس في يناير 2015، كان واضحًا للغاية أننا ننزلق في هذا. إلا أننا شعرنا أن هذا التزام بتحقيق ذلك خلال فترة معقولة. ولم يكن هذا تأخيرًا للأبد، فقد احتاج للعمل. لأن هذا هو الالتزام نحو لماذا علينا الثقة بهذا المفتاح. [غير مسموع] في هذا، ولدينا جميعًا مشكلة. نعم التالية.

فقط أقدم لكم خلفية صغيرة. ولدينا مفتاحان هناك في منطقة الجذر. فنحن لا نتحدث عن مفتاح الدخول لمنطقة الجذر. على أن مفتاح الدخول لمنطقة الجذر يتم استبداله بالفعل كل ربع سنة. لذا، في أول يناير وأول أبريل وما إليه، يتم استبدال المفتاح بصورة تلقائية. ويتم نشر المفتاح الجديد فحسب لفترة عشرة أيام، وتتغير المفاتيح في حين يستبعد المفتاح القديم بعد عشرة أيام أخرى.

كما تتم إدارة هذا المفتاح بالأساس من Verisign كجزء من إدارة الجذر في العمليات اليومية. الآن، سبب أنهم يمكنهم القيام بهذا هو أن هناك مفتاح لذلك. مفتاح الدخول الرئيسي. ويستخدم هذا المفتاح لتوقيع كل مفتاح دخول لمنطقة جذر جديد لذا هذا هو سبب تتبع المحللين السحري لتغيير مفتاح الدخول لمنطقة الجذر. ولا شيء تحتاجون القيام به، التالي.

يكون مفتاح الدخول الرئيسي مختلفًا بالطبع. فهو طرفي. وهذا هو الأمر الذي يحتفظ كل محلل تحقق من الصحة بنسخة منه على جهازه. كما أنه الشيء الموجود داخل الجهاز عند قيام الجهاز بعملية تحقق من DNSsec. لذا، فهذا جزء من بيانات التكوين العادية. والمفتاح الفعلي، الجزء الخاص من المفتاح يحفظ دون اتصال في منشآت آمنة للغاية. نعم التالية.

ولدينا الأضواء الشديدة وكلاب الحراسة وكافة هذه الأمور. نعم التالية. باستثناء في كاليفورنيا، حيث تكون الأمور أكثر هدوءً. نعم التالية. وقد اكتشفنا هذا في أمستردام. نعم التالية. لذا، المشاركون. إنها ليست فقط ICANN. فهي مجرد طرف. وضمن الترتيبات الحالية، تعتبر NTIA جزءًا من وزارة التجارة بالولايات المتحدة وهي أحد شركاء إدارة منطقة الجذر. وبالطبع، يشكل المشغل، Verisign، جزءًا من الشراكة أيضًا.

كما أننا تأسسنا السنة السابقة كفريق تصميم مع الزملاء من كل هذه المناطق للمساعدة في وضع تصميم بالفعل لكيفية وضع هذا المفتاح الخاص. نعم التالية.

لذا، هناك قليل من التاريخ في هذا الصدد، كما سمعتم من روس، وقد كانت هناك مشاورات مبدئية. لم يشارك فريق التصميم في 2012، دراسة هندسية في 13، مراجعة SSAC في 2013 وقد عمل فريق التصميم عبر معظم 2015. نعم التالية.

لذا، إذا كنتم ستتعرضون للتفاصيل، فكثير من العمل في الجزء المبكر من سنة النقاش، والنقاش والانتهاء حول الحدود، ولماذا. كذلك، قد ترون تعليقًا عامًا، مسودة مطروحة في أغسطس مع تعليقات تنتهي في أكتوبر، وهي أول جزء من هذا. وبعد ذلك من أكتوبر حتى نوفمبر، أعددنا التقرير النهائي. نعم التالية.

الآن، أول هذا هو طرح المفتاح وهو مهم لأن الجميع بالخارج لديهم نسخة من المفتاح الحالي. لذا، كيف نقوم بأتمتة حصول كافة الزملاء على المفتاح الجديد واستبدال القديم بالجديد؟ ليس هناك شيء فوق هذا. لا توجد طريقة تلقائية للقيام بهذا، حيث أنكم تعتمدون على آلية ثقة أخرى.

لذا، فهذا نوع من المشاكل والتي تمثل في أنه في حالة فهمنا الخاطئ، فسيكون للمحلل مفتاح قديم. ولكن، الأمر الذي نحاول التحقق منه يكون مسجلاً بمفتاح مختلف. ويسمى هذا فشل الخدمة، ومن ثم الوصول إلى طريق مسدود.

لن يقدم هذا لكم إجابة ويقول "لم أتمكن من التحقق من ذلك." لأنه يفهم البروتوكول، فهو يقول "شخص ما يلعب بكم. ولن أقدم إجابة." لذا، في هذه الحالة يكون الفشل في الأجهزة وليس البرامج. نعم التالية.

لذا، ما نقوم به بالفعل هو استخدام خدعة أخرى في التشفير وأنتم تعتمدون على حقيقة عدم وجود مفتاح يحقق حل وسط عند اقتراب الاستبدال. وهذا لا يعمل عند تعرض المفتاح. لذا، فنحن نفترض نوعًا ما الآن أن الأمور جيدة. وإذا كانت الأمور لا بأس بها، فالطريقة التي نطور بها الثقة في المفتاح الجديد هي تسجيله بالمفتاح القديم. كذلك، إذا كنتم تثقون في المفتاح القديم، ويسجل المفتاح القديم آخر جديد، فهذا المفتاح الجديد لا بأس به، أليس كذلك؟ لأنه المفتاح القديم هو من سجله.

إذن فهذه هي الآلية التي نستخدمها. وقد تم توثيقها بالفعل في RFC 5011، ولكن الطريقة التي تعمل بها هي نشر هذا المفتاح الجديد وإدراجه في منطقة الجذر، ولكنكم تسجلون هذا المفتاح بالقديم. وتتركون ذلك لفترة.

الآن، إذا كان المحللون مشاركين، وقد تم تكوينهم لتتبع استبدال المفتاح تلقائيًا، إذا كبيرة، فسيرون هذا المفتاح الجديد مسجلاً بالقديم، وسيكون الوضع "حسنًا. أفضل تحميل القيمة الجديدة وحفظها في ذاكرتي المحلية بجانب القديمة، والآن كلاهما موثوق به." بعد ذلك، نصل إلى النقطة الثالثة، حيث نسحب التوقيع القديم والمفتاح القديم، وبعدها في النهاية، لأنه بالفعل خطر أن نترك مادة قديمة موثوقة في المحلل.

لأنه عند التقدم لخمس سنوات ووضع المفتاح القديم، والذي تثقون به، فأنتم في موقف صعب. لذا، ما علينا القيام به بالفعل هو نوع من التنظيف العام وهي الخطوة الرابعة، مع إلغاء المفتاح القديم. لذا، نعيد نشر المفتاح القديم مرة أخرى، ولكن هذه المرة هناك جزء من التوقيع يقول "إذا كان في ذاكرة التخزين المحلية، فامسحه. فهذه نفايات. ولا تستخدم هذا المفتاح." نعم التالية.

لذا، هذه هي المراحل في النموذج البياني، وتأخذ هذه الأرباع الثلاثة، أي تسعة شهور. وهذا بطيء بصورة متعمدة. الآن، على الخط العلوي، يدور مفتاح الدخول لمنطقة الجذر كل ربع سنة. لذا، فهم ينشرون المفتاح القديم لعشر سنوات أخرى، قبل الانتقال إلى مفتاح الدخول لمنطقة الجذر لمدة 70 يومًا، وبعدها عشرة أيام أخرى، لنشر مفتاح الدخول لمنطقة الجذر. لذا، على القمة، فهذا الاستبدال المعتاد لمفتاح الدخول لمنطقة الجذر.

بأسفل الزر، عملية مفتاح الدخول الرئيسي الجديد. لذا، بالنسبة لأول ربع، في اليوم العاشر، يتم تقديم المفتاح الجديد. ولا يتم استخدامه، بل تقديمه. كذلك، في اليوم الأول من الربع التالين سيختلف المفتاح القديم فجأة. هل يداهمني الوقت، ولكن هذا مقصود. فالمفتاح القديم سيختفي، [thonk]. وكل ما لدينا حينها هو المفتاح الجديد، وكفى.

لذا، إذا عرفتم المفتاح الجديد حينها، فلديكم مشكلة. كذلك، سنشغل هذا لربع سنة كاملة وعشرة أيام، وبعدها يمضي كل شيء بصورة مناسبة، ثم تصبح الخطة إعادة نشر المفتاح

القديم وقول "عليكم تدمير النسخة المحلية. تخلصوا منها." عليكم القيام بهذا لمدة 80 يومًا إضافية للتأكد من وصول الرسالة وقد انتهينا جميعًا. نعم التالية.

لذا، فهذه هي الثلاث نقاط المهمة. قبل التحميل والتحول الحرج ونقطة اللا عودة مع الإلغاء. أليس كذلك؟ حسنًا، التالي. لذا، يفترض أن هذا سينجح، أليس كذلك؟ إذا قام الجميع بالأمر المناسب، فسيتم دعم RFC 5011 لدى كافة جهات التحليل. ويدعم الجميع ردود DNS الكبيرة لأن الردود ستصبح كبيرة، وسيمضي الجميع بدون دفع. نعم التالية.

وهذا هراء بالطبع. نعم التالية. لذا، المشكلة الأولى التي يعبر عنها بعض المحللين "أنا أدير مفاتيح الثقة المحلية يدويًا." لذا، فلا يهم ما نقوم به منطقة الجذر، حيث ستأخذ جزءًا من التكوين على الوحدة الطرفية لتغيير المفتاح. ولديهم مشكلة. فإما أنكم تهتمون أو ستضيعون. هذا أو ذاك. إذن هذه هي المشكلة الأولى.

أما المشكلة الثانية، فهي أن هذه الردود يتسع نطاقها. ويمكن أن تتعامل DNS بالتأكيد مع مجموعات كبيرة ولكن مسار الشبكة بين خوادم اسم الجذر المفوضة والمحليين قد لا يكون كذلك. كما قد لا تحصلون على إجابة. ويمكن ألا تتحمل الشبكة بالفعل هذه الردود الكبيرة. نعم التالية.

لذا، الأولى هذه المخاوف الفنية. وبعض المحللين لا يدعمون الاستبدال التلقائي للمفتاح. كم العدد؟ نحن لا نعرف. كم عدد المستخدمين؟ نحن لا نعرف. فماذا سيفعلون في حالة فشل التحقق؟ حسنًا، إذا كنتم تستخدمون محلل قديم، فسيذهب إلى مجموعة الاستعلامات، وسيحاول في هذه السنة ويحاول مرارًا وتكرارًا، ولدي دليل هنا على قيام المحللين بذلك. لذا، إن كنت ستنتقل إلى محلل جديد، فسيكون الرد "لا، هذا هو. لا فحسب، ولا توجد إجابة لأي سؤال. لا.

ماذا سيفعل المستخدمون عند رد المحللين بلا؟ حسنًا، بعضها سيذهب لعدم لمحلل لا يحل ولا يتحقق من الصحة. إننا نعرف ذلك. فلن يفعل ذلك 16% من المستخدمين. لا تعني لا، وهي تعني اللون الأسود في هذا الموقف. نعم التالية.

لذا، لا يمكننا اختبار هذا مقدمًا لكم. وقد حاولنا كافة أنواع الآليات لمعرفة كيف يمكننا التسلل لمعرفة ما يجري معكم ومع المحلل. ولا يمكننا التدخل في هذا الحوار. فلسنا نعلم ببساطة. وسنعرف ما يحدث. حسنًا. وهذه هي حقيقة الموقف. نعم التالية.

هناك الكثير من DNSsec هناك، لذا، نحن لا نتحدث عن أرقام بسيطة. لدى 87% من الاستعلامات DNSsec مناسبة. أتذكر من الاختبار هذا الصباح؟ إذا تم تسجيل المنطقة، سترد 87% من كافة الاستفسارات بتوقيع المنطقة. وهناك الكثير من DNSsec. على أن 33% من DNSsec استعلامات مناسبة تحاول التحقق من الصحة. ومرة أخرى، هذه أرقام كبيرة بالفعل.

بالأساس، نصف هؤلاء، عند العودة إلى فشل الخادم، سنذهب ونستخدم المحلل الذي لا يتحقق من الصحة، ولكن النصف الآخر سيبقى هنا ويقول "لا تعني لا." التالي. ردود DNS الكبيرة. ونعرف جميعًا أن شيئًا ما أقل من 1500 مجموعة ثمانية سيعمل بصورة مناسبة. أليس كذلك؟ هراء. لن يعمل، في UDP، بمجرد وصوله لحوالي 1350 مجموعة ثمانية، تصبح الأمور بطيئة للغاية. وما لاحظناه بالفعل في التجارب، ويمكن تجربته مع هذا، هو أن حوالي 6% من الاستعلامات تتعرض لتقسيم عند وجود 1350 مجموعة ثمانية للردود، وسيتم إجبارها على استخدام TCP.

لا يحب جميع المحللين استخدام TCP. محلل جدار الحماية والسياسات، مهما يكن، فهناك معدل فشل من 1% إلى 2%، وهذا سيء بالفعل. لذا، فستتسبب الردود الكبيرة في تلفيات. على الجانب الآخر، يشغل org. مفتاح DNS بمعدل 1650 مجموعة ثمانية. وليس لدي فكرة عن خبراتهم، فلا أحد يقول "يا إلهي، كان هذا رهيبًا. لقد فشلت للأسف." لذا، فقد وصلتنا معلومات التعارض هذه التي تقولها التجربة، "سيتعطل 1% إلى 2% من الزملاء عند 1350. في حين تبقى org. تعمل حتى 1650. وهذا هو الإنترنت، كل شيء ممكن في وقت واحد. وربما تكون قطة شرودينجر هنا." نعم التالية.

لا نعرف عدد الأصدقاء المستخدمين 5011 والتعامل التلقائي. ونحن سنرى هذا بالفعل عند طرحه. نعم التالية. لذا، بعض الأمور ستفشل. وسيتحول بعض الزملاء إلى محلل غير محقق، فبعضهم قد يوقف عمل التحقق من الصحة. كما سيخرج عدد صغير من الأصدقاء ببساطة بدون أي شيء. نعم التالية.

وستضع هذه الشرائح قليل قبل تغير الأحداث. كما أننا سنعرض بالفعل عليكم هذا التقرير قبل نشره لأني كنت متضايقًا قليلاً من حقيقة أنه لم يتم نشره، ولكن ICANN، للإشادة بهم، ونشر هذا يوم الاثنين. لذا، فعندما أقول أن المنشور لا يزال وشيكًا، وكانت هذه قصة الأحد. وقصة الأحد هي أنكم يمكنكم العثور على ذلك في مكان ما في موقع ICANN. هذا رائع.

نعم التالية. وهنا التوصيات التي كنت سأشاركها معكم. لذا، لم يعد سرًا أنها لا تزال مناسبة. وسأترككم لقراءتها، فهناك الكثير، ولن أتناولها جميعًا. نعم التالية. لذا، هناك أمرين هنا أود إبرازهما، بعد ذلك. نعم التالية. نقطة.

16. نقول إلى ICANN "هناك مقياس، يا إلهي، هذه المشكلة أسوأ مما اعتقدت." ونحن نقترح أنه إذا كنا سنحصل على أكثر من 0.5% من عدد مستخدمي الإنترنت المقدرين لا يزال متوقفًا لثلاثة أيام بعد الاقتراب من هذه النقاط الحرجة، فربما يكون هذا وقت التفكير بالفعل في دعم هذا على الفور. كما كان هذا الأفضل فيما كان ضررًا غير مقبولاً. لذا، 0.5% من عدد المستخدمين المتوقع تأثر سلبًا بعد ثلاثة أيام.

ويمكنكم الدفع بهذا، لكن هذا كان بالفعل [غير مسموع] مما شكل خطرًا على التقدم "ما مقياس الضرر؟" وقد بدا ذلك قياسًا معقولاً. نعم التالية.

صحيح. كان هذا بالفعل الإطار الزمني المقترح في هذا الوقت. ولم يتم نشره. فقد بدا 1 أبريل صعبًا بالفعل. فلا يزال هناك حولي 18 يومًا أو مهما يكن على هذا التاريخ. ولكن مع ذلك، ليس الأمر صعبًا بقدر ما يبدو. فأول تسعة شهور هي بالفعل احتفالات تسجيل المفتاح وإعداد مادة المفتاح الجديد. لذا، لا توجد تغييرات في المنطقة الجذر. لذا، لا توجد تغييرات في المنطقة الجذر. ولكن هناك تسعة شهور لفتح المفتاح بالفعل، والمراسم العادية في مجموعات التأمين، والتنقيب في الرمال، مهما يكن. القيام بهذا العمل ثم تغيير المفاتيح.

كذلك، تبدأ اللعبة الفعلية في الأول من يناير، وسيكون تغيير الجذر في العاشر من يناير. والمدهش في هذا الجدول المحدد، أن هذه، شريحة واردة وأخرى صادرة، ولا يوجد مفتاح قديم بعد ذلك في الأول من أبريل 2017. وهذه فقط الطريقة التي نجح بها الأمر، والموضوع برمته يجب أن ينتهي إذا مضي كل شيء جيدًا ولم يكن هناك ضرر حتى سبتمبر من هذه السنة بالفعل. نعم التالية.

لكن، ماذا ستفعلون؟ هناك شيء يمكنكم القيام به، وأكثر لتحقيق الهدف، وهناك شيء عليكم القيام به، التالي. إذا رأيتم هذا في تكوين المحلل، فعودوا إلى النوم. وأنت تبلون بلاءً حسنًا لأن المحلل ليس مفاتيح مدارة حاليًا. وستمضي الأمور. نعم التالية. لديك مشكلة. إذا رأيتم هذا، فعلكم الاهتمام. لأنه إن لم تهتموا، فسيتعطل عملكم. ولا يمكن لبقيتنا القيام بأي شيء حيال هذا. لذا، هاتان هما الشريحتان التي تمثل شرائح كبيرة بالفعل والتي أردت توضيحها لكم.

وإذا كنتم تستخدمون مفاتيح موثوقة، مفاتيح مدارة يدويًا، فعليكم الاهتمام بشدة للسنتين القادمتين. وإذا تغير الجدول الزمني، فتحتاجون لمعرفة هذا لأنكم قلتم أنها ستكون إدارة يدوية. وإن قمتم بإدارة تلقائية للمفاتيح، فلا بأس. وستمضي الأمور. نعم التالية. ها هي.

روس موندي: شكرًا لك جيوف. سننتقل بسرعة إلى وارين، ولكن شكرًا على العمل الرائع بالفعل. أردت فقط الانتقال إلى الأسئلة؟ حسنًا. يقول وارن أن جيوف غطى كل شيء أراد قوله، لذا، سننتقل ونتلقى أسئلة حول هذه النقطة. روبرت، هل رفعت يدك أولاً. تفضل.

روبرت مارتن ليجين: أجل. شكرًا. أنا روبرت مارتن ليجين، من PCH. حسنًا، بالنسبة لشريحة المفاتيح المدارة، يتطلب الأمر أيضًا أن [غير مسموع] تسجيل الملفات لأنها تقول في بعض الأحيان أنها تحتاج لملف لكتابة الموضوع فيه، وإذا لم تقوموا بتكوين هذا أو كتابة التصريحات، فلن يعمل هذا على أي حال.

فهل يمكنكم العودة، مهما يكن الأمر؟ نعود إلى شريحة الجدول الزمني ذات الألوان اللطيفة؟ وهناك الكثير من الشرائح. على أي حالي، كانت مخاوفي هنا في بداية الربع الثاني، أن نبدأ على الفور. وهي لا توضح متى نبدأ تسجيل المفتاح، فهي توضح فحسب موعد استبعاد المفتاح الأول.

جيوف هوستن: في الأول من أبريل 2017، سيتم تسجيل سجل موارد مفتاح DNS في منطقة الجذر بالمفتاح الجديد، وستكون محتويات هذه الموارد في نفس اليوم مفتاح الدخول لمنطقة الجذر الصادر وكذلك مفتاح الدخول لمنطقة الجذر الوارد، وأيضًا مفتاح الدخول الرئيسي الجديد. كما أن كل هذا موضوع للحد بفعالية من حجم الرد. وهذا هو المسار المصغر المطلق الذي لا يقدم معلومات متكررة في رد مفتاح DNS. كما أنه صغير بأقصى ما يمكننا فعله.

وبالرغم من هذا، عند الإلغاء في الربع الثالث. وعلينا تسجيل مفتاح DNS مع توقيعين. ويتم إلغاء أحدها والآخر لا. على أن هذه النقطة هي 1297 مجموعة ثمانية بجانب المقدمات. إذن ستكون هذه مشكلة.

روبرت مارتن ليجين: أفكر مثل تفويض TLD. وقد كان لديكم [RSSAC] وبها TTL. وعند البدء على الفور في تسجيل مفتاح الدخول الرئيسي الجديد، واستبعاد المفتاح القديم، مثلاً في الربع الثاني، كما أعتقد، ألن يكون لديكم تقرير مشكلات؟

جيوف هوستن: وسيتم تحميله إذا حصلتم على إدارة تلقائية للمفتاح الجديد في مجموعة المفاتيح الموثوقة. لأنها ستكون مجموعة المفاتيح الموثوقة، وستقبلون بسجل مفتاح DNS عند هذه النقطة.

روبرت مارتن ليجين: حسنًا، أتفق، ولكني لا تزال لدي uk. مع ست ساعات من TTL في المخزن المؤقت.

جيوف هوستن: ولكن .uk مسجل من مفتاح الدخول لمنطقة الجذر، وما إلى ذلك. إن كنت لا تمانع.

روبرت مارتن ليجين: ربما.

روس موندي: شكراً لك على هذا السؤال، روبرت. أجل. هذا أحد الأمور السحرية الرائعة، التي ينظر إليها في هيكل 5011. ولكننا نشجع هنا الحوارات المستقلة بدون اتصال. حسنًا. لست متأكدًا من أن هناك مزيد من الأسئلة أو التعليقات من الناس. أليس كذلك؟ لا؟ حسنًا. آه، نعم. تفضل. هناك. الاسم والانتماء من فضلك.

شخص غير محدد: اسمي [غير مسموع] وأنا من المملكة العربية السعودية، مركز معلومات الشبكة. لدي سؤال فيما يتعلق بالخوارزمية وطول المفتاح للجذر. هل سيتم تغييرها؟

جيوف هوستن: هل تتقدمون فحسب؟ وكانت لدي بالفعل بعض الأسئلة التي طرحتم. برجاء المتابعة. هناك بالقرب من النهاية. نقطة. عذرًا. تابع التقدم، أكثر. وسأقدم لك مكافأة لأنكم سألتم أحدها. شكرًا جزيلاً لكم. نعم التالية. هذه. أليس هذا صحيحًا؟

لقد طرحت هذا السؤال. فهل يجب القيام بتغيير الخوارزمية، أيضًا؟ هذا صحيح بالتأكيد أننا سنقدم مخاوف أقل إذا استخدمتم ECDSA لأن مشكلة المجموعة الكبيرة ستختفي. أليس هذا صحيحًا؟ إذا انتقلنا إلى ECDSA، فستكون الردود أصغر بكثير.

ونحن نتلاعب بالحوار ونغير أحد الأمور في كل مرة، ولكن مع مواجهة مشكلة المجموعة الكبيرة مقابل أسلوب أكثر عدوانية لتغيير البروتوكول بجانب تغيير المفتاح. وهذه هي المرة الاولى التي يتعرض فيها العالم لتغيير مفتاح الدخول الرئيسي. كما أخطأ فريق التصميم على جانب الحوار وكذلك في الردود الأكبر. كذلك، طالما أن كل شيء لا يزال كما هو، بما في ذلك حجم مفتاح الدخول لمنطقة الجذر، وهو الأمر المهم للغاية، فإن الضرر سيكون في أقل درجة، ولكن لا يزال لا بأس به، كما أعتقد.

وإذا أصبح مفتاح الدخول لمنطقة الجذر أكبر، فستكون الردود أكبر، وندخل في مشكلة أخرى. لذا، نعم، فكرنا في هذا، وشعرنا أننا لا يمكننا تجاهل ECDSA، لكننا يجب أن نطرح المفتاح أولاً على الأقل للحصول على بعض الخبرة حول كيف يبدو، وبعدها لدينا مجموعة لاحقة تنظر في استبدال البروتوكول. شكرًا.

روس موندي: نعم. وفقط للإضافة إلى رد جيوف هناك، تم إدراج SSAC 63، وقد ناقشنا هذا داخليًا. كذلك، لا توجد تفاصيل بالتحديد حول هذا الأمر، ولكن كانت النتيجة النهائية أن هناك سطر أو اثنين في التقرير تقول "يجب أن نقوم باستبدال المفتاح أولاً." لذا، ستكون نفس النتيجة من SSAC كفريق التصميم حيث يترتب على استبدال المفتاح لاحقًات تغيير الخوارزمية. شيء واحد في كل مرة.

شخص غير محدد: ماذا عن طول المفتاح؟

روس موندي: في هذه الفترة الزمنية، فترة SAC 63، لم يتم التعامل مع هذا، لذا، فلم يتم النظر فيه على الإطلاق.

جيوف هوستن: كما أن مفتاح الدخول الرئيسي هو 204 لمفتاح 8 بت. لذا، لم نشعر أن النصيحة التي تلقيناها من كافة الزملاء في التشفير وهذه النصيحة في التقرير بدا كما لو أنه كانت هناك حاجة لتغيير طول مفتاح الدخول الرئيسي في هذا الوقت. كما كانت هناك بعض المناقشات الموازية حول مفتاح الدخول لمنطقة الجذر 1024 بت، وهذه المشكلة بالكامل التي طرحتم أولاً ولماذا؟ وما هي تداعيات تغيير مفتاح الدخول لمنطقة الجذر وليس مفتاح الدخول الرئيسي؟

روس موندي: مرة أخرى، أحد الموضوعات المهمة للغاية هي الحاجة لمراقبة الأشخاص وإدارتهم ومراقبة الأنظمة بعناية شديدة مما يستلزم التواصل مع الآخرين، ويحتاج الناس لمعرفة الأمور التي عليهم مراقبتها. لذا، وارن.

وارن كوماري: إذن نعم. لقد كنت أحد المؤلفين الأصليين مع روس في SAC 63. لذا، كانت هذه نغمة رائعة. شكرًا، شكرًا. وأعتقد أنني اتفق مع كافة التوصيات المطروحة. مع ذلك، جدير بالذكر أن عددًا من الوثائق الأخرى كان مماثلاً للغاية أو مطابقًا تقريبًا للتوصيات بالكامل الواردة في SAC 63. وكانت هناك على الأقل اثنين من فترات التعليق العام، وقد تضمنت بالأساس نفس مجموعة الأمور.

كان هناك اجتماع إدارة ملف خادم الجذر. وقد تضمنت النسخة الأصلية من الوثيقة من فريق التصميم بالأساس نفس الأمور. لذا، أعتقد أنه من المثير ملاحظة أن الفريق الفني يبدو أنه في نفس الصفحة، والتي تنص بصورة كبيرة على أنه مهم، على أننا نحتاج للقيام به والتقدم فيه، وأعتقد حتى الآن أن لدى الجميع كافة التقارير التي اقترحت أن نتمسك بها مع RSA للوقت الراهن و2048.

روس موندي: أسئلة أخرى. حسنًا. آه، نعم، دان. تفضل.

دان يورك: أود فقط أن أوجه خالص الشكر إلى فريق تصميم مفتاح الدخول الرئيسي الذي قضى الكثير من الوقت والساعات في تجميع هذه الوثيقة. إذن. بول ووترز هنا. هل هناك أحد هنا، بول، الذي تتذكروه من فريق التصميم؟ لقد غادر أوندريج. وهو بالخارج للاستمتاع بأضواء المغرب ولكن نعم، نيابة عن نفسي، بول وأندريج، شكرًا جزيلاً.

وارن كوماري: حسنًا، أرى أننا لا يزال لدينا بعض الوقت، وسألعب دور محامي الشيطان.

روس موندي: لا، لن تفعل.

وارن كوماري: لذا، تقول أن 16% من الأشخاص لن يتمكنوا من حل الإجابات غير الصحيحة في الوقت الحالي، في حالة فشل DNSsec. وقد حصلتم بالفعل على بعض الأمور التي تقول أن هناك بضعة محللين كبار، يقدمون خدماتهم لمجموعة من الأشخاص. كما نتمنى أن نقوم باستبدال المفاتيح بصورة صحيحة. ولكن، لا يزال هذا، يترك عددًا كبيرًا منه الناس ربما في خطر.

ويقول فريق التصميم أن 0.5% بعد ثلاثة أيام هي نسبة مقبولة. ويبدو هذا رقمًا كبيرًا للغاية للأشخاص الذين لن يتمكنوا من تشغيل DNS. كيف توصلتم إلى ذلك؟ وأقول، ألعب محامي الشيطان، للاستفزاز.

جيوف هوستن: انظر، سيكون من اللطيف بالفعل أن أقول صفر. أليس هذا صحيحًا؟ لا ضرر بعد ثلاثة أيام، فقط كل شيء يعمل بصورة مناسبة أو نعود. ولا أعتقد أن هذا واقعي ضمن التكنولوجيا والتنوع الذي نراه هناك. حتى الآن، هناك قدر ما من الضرر في DNSsec يحدث الآن. وربما لم يكن معقولاً.

فنحن، كما أفترض، نخاطر للغاية هنا، بقول إن أمكننا قياس هذا، نحتاج لأن يكون في نقطة يمكن قياسها بصورة واضحة. ولست متأكدًا من أننا يمكننا قياس الإنترنت بمستوى تفصيل أكبر من 0.1%. وأقل من ذلك، يعتبر مجرد تشويش. كذلك، لن يكون قياسًا موثوقًا. لذا، كان هذا نوعًا من أننا يمكننا القياس والمعرفة في إطار زمني كان معقولاً.

كان هذا الموضع الذي وصلنا إليه بسبب أننا تماشينا مع الأمور. وإذا كان هذا مستوى الضرر، فيجب أن ندعم ذلك بالفعل. كذلك، هذا هو ما وصلنا إليه، ولكن هذا يتعلق بمقدار العلم وراء هذا.

روس موندي: أود أن أشكر كافة الأعضاء هنا وأدفع كل من في القاعة للنظر في عناوين URL، والامساك بالوثائق، على الأقل الاطلاع عليها، وربما قراءتها بالتفصيل. كذلك، توجد بعض المعلومات المفيدة ومن الجيد أن يدرك الزملاء محتواها. شكرًا لك جيوف. شكرًا لك، وارين.

دان يورك: لا بأس بنا. مرحبًا. حسنًا. نحن في المرحلة الأخيرة من ذلك. كما أود أن أشكر جميع الموجودين هنا. وأنا أرى الكثير منكم منذ التاسعة صباحًا، لذا، دعونا نصفق لأنفسنا. لذا، نريد فحسب تلخيص كيف يمكنكم جميعًا المساعدة، واقتراحاتنا، وما نود طلبه من الجميع هنا، وعادة ما أعمل أنا وروس على هذا، ولذا، سأغادر في النص الأول، ولكني سأقول إذا كنت مشغل TLD، أو ccTLD، فنحن [غير مسموع] نطلب منك تسجيل النطاق.

لقد سمعنا عبر اليوم عددًا من مختلف الموارد المتوفرة، بما في ذلك إذا كنتم هنا في المنطقة الأفريقية. كما أن لدينا الزملاء من AFRINIC، الراغبين في القدوم والسفر وعقد ورشة عمل في الجلسة. وإذا لم تكونوا في أفريقيا، فهناك موارد أخرى من ICANN التي ستقوم بنفس نوع ورشة العمل التي ستتمكن من مساعدتكم بها.

كما نطلب من الناس قبول سجلات DS للعمل مع أمناء السجل ومساعدتنا أيضًا في الإحصائيات. وقد رأيتم المخطط هناك سابقًا مع قائمة إحصائيات ريك لامب حول عدد النطاقات مقابل المسجل. كما نود التأكد من أن ذلك يتضمن كافة نطاقات TLD ذات الصلة، والموجودة هنا. لذا، نطلب من مشغلي ccTLD القيام بهذه الخطوات. وأعتقد، تفضل روس.

روس موندي: لذا، مشغلي المنطقة الآخرين بجانب مشغلي TLD. وإن قمتم بتشغيل الخادم المعتمد في DNS، فانظروا في استخدام DNSsec له. ليس الأمر بهذه الصعوبة بالفعل. وكما سمعتم اليوم، هناك مقدار ضخم من المساعدة والدعم والموارد التي يمكنكم الاستفادة منها. كما يميل الأشخاص في هذا المجتمع إلى المساعدة للغاية. لذا، إذا انتقلت إلى شيء يتضمن مشاكل، فيمكنكم العودة والنظر في ورش العمل هذه ومعرفة من تحدث عن ماذا، وستكون لديكم ضمانة أنكم إن أرسلتم رسالة بريد إلكتروني، فستحصلون على رد والكثير من المعلومات المفيدة.

ومرة أخرى، الإحصائيات مهمة. كما أننا ننظر بالفعل في تجميع بيانات فعلية أكثر واقعية حول ما يجري على أرض DNSsec.

دان يورك: وإذا كنت أحد مزودي خدمات الشبكة، ISP، فيسعدنا أن نتطلب منك تشغيل التحقق من الصحة. كما نود أن نرى مخطط جيوف يصعد أعلى وأعلى. ونود أن نرى مزيد ومزيد من التحقق. فهذا مهم للغاية، جزئيًا، لأننا نحصل على بعض الدفعات، من بعض الشركات هناك عند الحديث إليهم عن التسجيل، فهم يقولون "حسنًا لماذا يجب التسجيل؟ لأنه لا أحد يتحقق."

وبعد ذلك، يشير إلى إحصائيات جيوف، شكرًا لك جيوف، ونقول، "انظروا، في هذا المخطط. انظروا في المنطقة الخاصة بكم بشأن مقدار التحقق الحادث. وليس هذا أحد الوحوش الأسطورية. وهذا أمر مهم حقا. كما أنه حقيقي." نحتاج إلى أكثر من هذا. حيث نريد التقدم مما نحن عليه الآن، 14% - 15% الآن على المستوى العالمي، ونريد إحضار ذلك حتى أعلى وأعلى.

هذا أمر بسيط. فعليكم فقط إتاحة، هناك بضعة خطوط في ملف التكوين، ولكن عليكم أيضًا العلم بأنكم يمكنكم التسبب في عدم تمكن الناس من الوصول إلى موقع الويب، لذا، فعليكم إعداد فريق الدعم وما إليه، للتمكن من دعم هذا، حيث أنا أسرع وأدرك حاجتي للإبطاء. وضحيتي هناك.

الجزء الآخر هو تسجيل المناطق والجزء الآخر ÷و أننا نود منكم الارتقاء بدعم بروتوكول DANE، الذي لم يتحدث بالفعل عن هذا هنا. ونحن نشجع الناس على القيام بهذا. ووارن يبتسم. روس.

روس موندي: لذا، إذا كنت مزود موقع ويب، ومزودي المحتوى الآخرين، فانظر في تسجيل كافة المناطق الخاصة بك. وإذا كنت مشغل موقع ويب، فهناك فرصة مناسبة أنكم إذا كنتم تتولون تشغيل موقع الويب الخاص بكم، فربما تشغلون دعم DNS. لذا، إذا كنتم تستعينون بمصادر خارجية لتشغيل موقع الويب مع تقديم المحتوى فحسب، فعليكم الذهاب إلى من يشغل الجهاز المحدد بالفعل. وعليكم إخبارهم أنكم تريدون تسجيل كل هذا وتريدون دعم DANE.

لذا، تريدون رؤية كافة هذه الأمور مفعلة والانتقال إلى الموردين. وعليكم التأكد من علم الموردين بحقيقة أنكم تريدون القيام بهذا. والشكر موصول طوال الوقت لأن هذا أصبح أسهل بسبب دعم مزيد من الموردين له. لكن، أحد المشكلات التي نواجهها لعدد من السنوات هي أن الموردين سيعوون لنا ويقولونه "لا أحد يسألنا عن هذا." ومثل هذا الرد عندما نتحدث عن التحقق، فلا أحد يسأل عن التحقق أيضًا.

ولا أحد يسأل عن تسجيل DNSsec. لذا، عليك طلبها من موردي كافة الخدمات التي تشتريها.

دان يورك: لذا، في النهاية، عندما يتمكن الجميع من القيام بهذا، فنحن نطلب منك استخدام DNSsec بنفسك. استخدم التحقق إن أمكنك، وإن أمكنك تشغيل هذا لتسجيل النطاقات، فقم بكافة هذه الأمور، مهما يكن ما يمكنك فعله بأي صفة تحملها. والأمر المهم أننا سنطلب منكم مشاركة الدروس المستفادة. وقد سمعنا بعض -- عليكم مشاركة الدروس المستفادة من خبراتكم. كما سمعنا أمور رائعة هنا، وسمعناها في اليوم الفني، وكذلك في أماكن أخرى. لذا، أود طرح الأفكار هنا.

ستكون الجلسة التالية في ICANN 5، في موعدها، على أننا ستكون لدينا جلسة أخرى لاحقًا في هذه السنة في ICANN 57. وسوف ننطلق من تلك النقطة. نعم، لقد فعلنا. لكن، كما تقوم جولي، يحدث الأمر الرسمي عند تصويت مجلس الإدارة، ولكنه قد يكون في فنلندا. لذا، على أي حال، متى يكن.

وسيكون لدينا لجنة إقليمية، عندما تبدأ الجلسات، كما نود إدراج الأشخاص على المستوى الإقليمي حيث كان الناس من أفريقيا في هذا، وسكون لدينا أشخاص من أي قارة في المرة القادمة. ونود إدراج الناس هناك. ونريد أن تقوم بهذا.

لذا، كان لدي أيضًا طلب اليوم، فقط سأل أحدهم "حسنًا، هل هناك طريقة للاطلاع على المستجدات أو التواصل مع الأشخاص الآخرين من وقت لآخر؟" وعلي أن أذكرن وقد قدمت ملاحظة لإدراجها بهذا للمرة التالية، فهناك قائمة بريدية والتي تسمى قائمة تنسيق

DNSsec ويمكنكم الانضمام لهذه القائمة ومشاركة المعلومات مع كل منهم الآخر. كذلك، لدينا أيضًا مكالمة هاتفية شهرية أول خميس من كل شهر باستثناء هذا الشعر حيث ساءت الأمور.

مع ذلك، عادة، معظم الشهور، إنه أول خميس من كل شهر عند التجمع في مؤتمر هاتفي والحديث حول ما هذه المشكلات، وكذلك الحديث عن كيفية تسريع النشر، والقيام بذلك. ونرحب بانضمام أي شخص. كما أن عليكم ببساطة الانضمام إلى القائمة البريدية حتى تعرفوا هذه الأمور. ويمكنكم العثور على مزيد من هذا هناك.

أود أن أشكر بضعة أشخاص مرة أخرى. حيث أود توجيه الشكر إلى رعاة حدث اليوم، Afilias و[سارة] ودين وSIDN. كما أود أن أشكرهم جميعًا وأود أن أقدم لهم جولة من التصفيق. في هذا الصدد، سأوضح أننا ننظر مرة أخرى في ممول آخر فقط لمساعدتنا فيما تبقى من 2016. وسيساعدنا هذا في متابعة القيام بهذا. كما أننا نتطلع بالفعل إلى ممول لتجميع جهات التنفيذ، تجمع مساء الاثنين في مكان الانعقاد الذي لدينا لاحقًا. لذا، ربما يجب علينا التفكير بذلك. فهل سترغب الشركة في مساعدتنا لمتابعة هذه الأنشطة التي تشكل جزءًا من هذا؟

وأرد أن أشكر بصورة خاصة جولي وكاثي اللتان ساعدتا في علم كل هذا بسلاسة كما هو. وبهذا، سأنتهي فقط بقول أنه إذا كنتم ترغبون في مزيد من المعلومات، فهذه بعض مواقع الويب التي يمكنكم الاطلاع عليها. DNSsec-deployment.org. مجتمع الإنترنت، ولن نصلح هذا أبدًا، org/deploy360. حسنًا.

لجنة البرامج، هل يمكننا جميعًا الاتفاق على حاجتنا لإصلاح هذا؟ كما نرى دائمًا أن هذه نهاية الجلسة ويمكنكم إرسال، حسنًا. لذا، هذا مجتمع الإنترنت. حسناً؟

شخص غير محدد: لأقل من 200 ألف دولار.

دان يورك: عذرًا، إنه internetsociety.org/deploy360. وبعدها، هناك أيضًا أدوات DNSsec. ومن موقع Deploy360، هناك رابط إلى مجتمع DNSsec، حيث سنعثر على هذه القائمة البريدية والأمور الأخرى، وكذلك الإحصائيات والموارد والمزيد الموجود هناك. وأود أن أتقدم لكم جميعًا بالشكر و --

روس موندي: كما أوجه الشكر الجزيل أيضًا إلى فريقنا الفني هنا والمترجمين لدينا. شكرًا جزيلاً لكم.

دان يورك: نعم. شكرًا للمترجمين. نعم. للاختصارات وسرعة الحديث وكل شيء آخر، فقد عانوا من الكثير اليوم. وربما يمكنهم الذهاب على أي حال. حسنًا، بهذا، نحتاج للإيجاز وأعتقد ربما أن علينا الخروج من القاعة بسرعة. لا أعرف. 15 دقيقة. حسنًا. لذا، نحن جميعًا بخير. شكرًا لكم جميعًا. أتمنى أن أراكم في اجتماع ICANN 56.

[نهاية النص المدون]