برشلونة – الامتدادات الأمنية لنظام اسم النطاق DNSSEC للجميع: دليل للمبتدئين
الأحد، الموافق 21 تشرين الأول (أكتوبر) 2018 – من الساعة 03:15 م إلى 04:45 م بالتوقيت الصيفي لوسط أوروبا
ICANN63 | برشلونة، إسبانيا

ويس هارداكر: ... يجعل العالم كله آمنًا إذا كنت تستخدمه وقمت بتشغيله. سوف نقوم بذلك من خلال قصة. سنبدأ بأصول DNSSEC، التي بدأت قبل 5000 سنة قبل الميلاد، أي قبل زمن بعيد جدا. وقد بدأت DNSSEC قبل ظهور الإنترنت بالفعل.

نقدم لكم أغوينا. وهي تعيش على حافة جراند كانيون. وبالنسبة لأولئك الذين ليسوا على دراية بغراند كانيون، فهو ثقب ضخم وسط الولايات المتحدة.

وهذا أوغ. يعيش في كهف في الجانب الآخر من جراند كانيون. بينهما مسافة كبيرة سواء عبر المنحدر أو عبر السفح، لذا ليس باستطاعتهما أن يجتمعا كثيراً للتحدث. وقد جربت ذلك. يمكننا بدء استخدام إشارات الدخان والمحادثة من جانب إلى آخر.

في إحدى زياراتهما النادرة لبعضهما، لاحظا أن الدخان يتصاعد من النار التي أضرمها أوغ. وبعد قليل، بدآ يتحدثان بانتظام باستخدامهما لإشارات الدخان عوض بروتوكول مخطط بيانات مستخدم الإنترنت UDP. وفي أحد الأيام، انتقل رجل الكهوف المزعج كامينسكي إلى جوار أوغ، وبدأ هو الآخر في إرسال إشارات الدخان. بالنسبة لأولئك الذين لم يكونوا هناك منذ حوالي عشر سنوات أو أكثر، كان كامينسكي هو المكتشف الحقيقي الذي اكتشف نقطة ضعف كبيرة جدًا في نظام اسم النطاق DNS.

والآن، نجد أن أوغوينا مرتبكة حقاً. فهي لا تدري ما هي الإشارات التي يجب عليها أن تصدقها. وبدون استعمال المنظار لتحديد من يرسلها، أي واحدة من إشارات الدخان البعيدة جداً يجب عليها أن تقرأها؟

وهكذا، انطلقت أوغوينا من الوادي محاولة بذلك تسوية الفوضى كلها. تشاور أوغوينا وأوغ مع كبار حكماء القرية. كان رجل الكهف ديفي يعتقد أن لديه فكرة ماكرة. بالنسبة لأولئك الذين لا يعرفون، كان ديفي أحد الأشخاص الذين أنشأوا تشفير المفتاح العام، والذي يعتبر اليوم أساس الكثير من علم التشفير داخل الإنترنت.

و في لمح البصر، قفز رجل الكهف ديفي و ركض هارباً داخل كهف أوغ. خلف ذلك الكهف، وجد هذا الرمل الأزرق الغريب الذي تم إيجاده فقط في كهف أوغ. وبقفزة منه، اندفع ورمى ببعض الرمال السحرية على النار، فتحولت إلى دخان أزرق رائع.

والآن يمكن لأغوينا وأوغ الدردشة بسعادة مع بعضهما البعض مرة أخرى، آمنين أنه لا أحد يستطيع أن يتدخل في محادثاتهما، لأن أوغ هو الوحيد الذي يملك الرمال الزرقاء السحرية.

إذن، هذا هو تمهيد DNSSEC في شكل رسم مبياني مبسط. لذلك، دعونا نعود إلى DNS قليلاً لأنه يعمل بطريقة مشابهة بالفعل لإشارات الدخان.

توجد بنية شجرية في DNS، كما يسميها البعض، أو تسلسل هرمي. يبدأ الأمر بالجذر من الأعلى. ثم تقع جميع TLDs أسفله. ويتضمن ذلك ccTLDs و gTLDs و TLDs الجديدة. ويوجد تحت كل واحدة منها نقاط تسجيل تحدث فيها أشياء مختلفة.

لذلك، سأشير إلى المنتصف في الأسفل، وهو bigbank.com. سوف نتحدث حول ذلك عدة مرات. إذن، يفوض الجذر com معلومات إلى خوادم com، وتفوض خوادم com bigbank إلى خوادمهم.

عندما يحاول أي محلل الإجابة على طلبك ربما في موقعwww.bigbank.com، نجد أنه لا يعرف الشجرة بأكملها. لذلك يجب عليه البدأ من القمة. ولكنه، يعرف مكان منطقة الجذر، كما أنه قادرعلى اجتياز التسلسل الهرمي لـ DNS من أجل أن يعثر عليه.

فكل مستوى في هذا التسلسل الهرمي، كما قلت، يشير إلى المحلل الذي بعده. لذلك، نجد أن المحلل يستطيع ببساطة اتباع السلسلة على طول الطريق حتى يتم الإجابة على السؤال في النهاية.

يقوم المحلل بتخزين كل تلك المعلومات للاستخدام المستقبلي. فبمجرد حصوله على هذه المعرفة، يمكنه أن يجيبك بسرعة أكبر لفترة من الوقت لأن باستطاعته تخزين المعلومات طالما أنه قادر على ذلك.

ومع ذلك، توجد هناك مشكلة مع DNS. لم يتم تصميمها بأي شكل من أشكال الأمن. تماما مثل إشارات الدخان التي لم يكن لديها أمن يحميها، وحتى DNS لم يكن لديها ذلك. إنها فقط تفترض بشكل ساذج أن كل شيء على ما يرام. يتم انتحال الأسماء بسهولة، فبالنسبة لتلك المخابئ التي

تستطيع أن تتذكر الأشياء لفترة طويلة، إذا حصلت على إجابة سيئة في ذاكرة التخزين المؤقت، سوف تتذكرها لفترة طويلة من الزمن أيضاً.

و نظراً لأن الرسومات التوضيحية المبسطة لم تكن مبسطة بما يكفي، سوف نقوم بعمل مسرحية هزلية. هذا هو المكان الذي يصبح الأمر فيه أكثر متعة. كم عدد الناس الذين شاهدوا هذه المسرحية من قبل؟

إثنان منكم. حسنًا. سيكون البقية على موعد مع المتعة. العدد القليل منكم الذين رأو المسرحية من قبل سوف يضطرون إلى المعاناة ومشاهدتها مرة أخرى.

حسنًا. هل يمكن للاعبي المتطوعين الوقوف من فضلكم؟

إذن، لدينا هنا عدداً قليلاً من اللاعبين. لدينا مستخدم متوسط، المستخدم جو. ارفعوا أيديكم رجاءً. سوف يكون هو المستخدم في هذا السيناريو، وسيحتاج إلى القيام ببعض الأعمال المصرفية اليوم. لدينا ممثل القاعدة الذي يمثل جذر شجرة DNS. ولدينا مزود خدمة الإنترنت ISP الذي يعرف مكان الجذر. كما لدينا كل من dot-com، و bigbank.com. في الواقع، أعتقد أنك محق على الأرجح في هذا الشأن، فريد. لذلك، سأدع لهم الكلمة هنا لنشرع في الأمر. هيا.

شخص غير محدد: [عندما] يومض الضوء، مرحباً، مرحباً.

ويس هارداكر: حسنًا، هيا لنبدأ. حسناً، كلاهما يعملان. تفضل، تيم. لدى روس الاستفسارات.

تيم: يا للعجب! لدي كل هذا المال. يجب علي تسجيل وديعة. أريد أن أذهب إلى www.bigbank.com لإيداع أموالي.

شخص غير محدد: حسنًا، أنا لا أعرف مكانه، لذلك سأذهب لأكتشف الأمر لأجلك. إذن، سوف أبدأ بالجذر. مرحبا، هل تعرف أين يوجد www.bigbank.com ؟

فريد بيكر: يا للعجب. ليست لدي أدنى فكرة. ومع ذلك، لقد حصلت على صفقة لأجلك! يمكنك أن تسأل dot-com، لعل dot-com بوسعها معرفة ذلك. إنه في 1.1.1.

تيم: ممتاز جدًا. سوف أعطيهم فرصة.

ويس هارداكر: [غير مسموع]. ها نحن ذا. عذرًا.

تيم: لقد قيل لي أن أسألك. هل تعرف أين يوجدwww.bigbank.com؟

شخص غير محدد: هذا سؤال رائع في حقيقة الأمر. أنا dot-com. أنا في الـ 1.1.1. شكراً على زيارتنا. ويمكنني أن أخبركم أي يوجد bigbank. ها نحن نبدأ. Bigbank هو 2.2.2. أترغب بالذهاب إلى هناك؟

تيم: شكرًا. أريد أن أعرف أين يوجد.www.bigbank.com

روس موندي: وشكراً لك السيد ISP على سؤالك. في واقع الأمر، يمكنني أن أخبرك بالضبط أين يوجد .www.bigbank.comإنه في 2.2.2.3.

تيم8: شكرًا. يوجد Bigbank.com في 2.2.2.3. رائع! يمكنني المضي قدما وإيداع أموالي! شكراً لك!

فريد بيكر: لا أدري. يجب عليه أن يشكركم.

ويس هارداكر: حسنًا. شكراً لكم جميعاً. إبقَ جانباً لأننا سنحتاجك مرة أخرى خلال دقيقة.

شخص غير محدد: لا تترك وظيفتك اليومية!

ويس هارداكر: هذا هو عملهم اليومي. لذا، فإن دردشة أوغوينا، وحدة الحل، مع أوغ ،الخادم، شبيهة بما شاهدته للتو. كانوا يتواصلون عبر إشارات الدخان. ولم تكن أي مشكلة آنذاك. لكن لم يكن هناك أي أحد يعبث معهم.

سوف نرى النتائج التي ستنجم عن ذلك لاحقاً عندما تسوء الأمورفي حال من الأحوال. هل يمكنم يا رفاق تكرار أدائكم؟

تيم: يا للعجب! لدي الآن مليون دولار، وأحتاج إلى إيداع هذه الأموال. أحتاج إلى الانتقال إلى www.bigbank.com، لذلك سأذهب إلى ISP وسأسأل: "كيف يمكنني الوصول إلىwww.bigbank.com؟"

شخص غير محدد: ليس لدي أدنى فكرة، لكنني سأحاول. مرحبًا. هل تعرف أين يوجدwww.bigbank.com؟

فريد بيكر: حسنًا، أنا الجذر، وأنا لا أعرف حقاً عن مثل هذه الأشياء. ولكن، يمكنك أن تسأل دوت-كوم. يمكن أنه يعرف ذلك. إنه على 1.1.1.1.

تيم: حسنًا. شكرًا. أنا dot-com. هل تعرف أين يوجدwww.bigbank.com؟

شخص غير محدد: مرحبًا. أنا dot-com. ويمكنني أن أخبركم أين يوجد bigbank.com. إنه في 2.2.2.

شخص غير محدد: 2.

شخص غير محدد: 2.

شخص غير محدد: بروتوكول الإنترنت- الإصدار الثالث؟

تيم: شكرًا. مرحبًا

شخص غير محدد: مرحبًا.

تيم: مرحبًا. هل تعرف أين يوجدwww.bigbank.com؟

شخص غير محدد: أعرف بالتأكيد. إنه في 6.6.6.6.

تيم: ممتاز جدًا. شكرًا. [غير مسموع]

شخص غير محدد: ها نحن ذا. www.bigbank.com يوجد في 6.6.6.6.

شخص غير محدد: يا الهي! شكراً! أريد أن أذهب لإيداع أموالي!

شخص غير محدد: شكرًا.

ويس هارداكر: حسنًا. شكراً مرة أخرى. لذا، فإن السؤال الحقيقي هو، كيف سنخرج من هذه الجلسة الرهيبة مع د. إيفل الذي يترأس كل الأبناك.

والآن، المحللة أغوينا مرتبكة حقاً. هذا هو الوضع الذي رأيته للتو. هناك إشارتان. فهي لا تدري ما هي الإشارات التي يجب عليها أن تصدقها. في الواقع، بالنسبة لـDNS، الذي يعود أولاً هو عادة الشخص الذي تؤمن به، كان هذا موجوداً على الأقل حتى مجيء DNSSEC.

و لذلك مجدداً و بالعودة إلى نفس الرسم البياني، إذا كان هناك خادمان مختلفان يقدمان لك إجابتين مختلفتين، فقد تحصل على جواب bigbank.com من مكانين مختلفين، ولن تعرف أي شخص تصدقه. لذلك، في الرسومات التوضيحية، هناك الزرقاء والحمراء. عليك أن تخمن ما هي الإجابة الصحيحة فقط.

ولكن، تقوم DNSSEC في الواقع بوضع رجال الأمن على DNS، وتستخدم التوقيعات الرقمية للقيام بذلك. إنه يضمن لك شيئين أساسيين، أولاً أنه لم يتم التلاعب بهذه المعلومات، ثانياً أنها

نشأت من المكان المناسب. لذا، بغض النظر عن عدد الأماكن التي تم تخزينها فيها، وبغض النظر عن مخابئها، لم يتم التلاعب بها وتستطيع التعرف من أين أتي بها أيضاً.

المفاتيح والتوقيعات مخزنة في DNS كذلك. نظراً لأن DNS لديه نظام بحث، يمكن البحث عن المفاتيح بسهولة، بالإضافة إلى التواقيع، تمامًا مثل أي يوم آخر، طالما كان لديك مكان للبدء.

لذا، فإن المفهوم ذو المستوى العالي لـDNSSEC هو أن المحلل لا يعرف مكان خادم الجذر فقط، بل أيضًا مفتاح خادم الجذر. طالما أنه يعرف ذلك، أي أنه يعرف تلك القطعتين المتعلقتين ببداية المعلومات، يمكنهما التحقق من بقية الشجرة.

فهو يفعل ذلك عن طريق بناء سلسلة من الثقة. كل مستوى يوقع المستوى الذي يليه والبيانات التي تشارك في مستواها الخاص، حتى يتم إكمال السلسلة على طول الطريق للحصول على الإجابة التي تحتاجها.

أخيراً، وبهذه الطريقة، تستطيع وحدة الحل في ISP تحديد أي زر من هذين الزرين الخاصة بتسجيلات bigbank هو الأصح، فالصحيح يكون أزرقاً، وX يشير إلى السيء.

لنرى ما يحدث بالفعل مع DNSSEC في اللعب. هناك شيئان سنقوم بمواجهتهما اليوم. و الآن يمكنك رؤية هذه الميداليات القليلة. هذه تشير إلى التوقيعات الرقمية. سيحصل كل خادم من خوادم DNS الثلاثة على هذه الميدالية، ومن ثم سيحصل ISP على ميدالية مطابقة للتأكد من أنه يستطيع التحقق بأنه يتحدث إلى الشخص المناسب. قدم ذلك القسم.

تيم: يا للعجب! لدي إيداع آخر. أنا بحاجة للذهاب إلى www.bigbank.com لتفعيل هذا الإيداع..

شخص غير محدد: حسنًا. سأبحث عن ذلك لأجلك.

مرحبًا بالجذر. من فضلك هل بإمكانك أن تخبرني بمكان www.bigbank.com؟

فريد بيكر: حسنًا. أنا هو الجذر، كما أنني أستطيع إثبات صحة تصريحاتي. ولكن، ليس لدي أي فكرة عن مكان bigbank. ولكن، يمكنك أن تسأل dot-com. إنه على 1.1.1.1.

تيم: شكرًا. أنا dot-com. من فضلك هل بإمكانك أن تخبرني بمكان www.bigbank.com؟

شخص غير محدد: أهلا، ISP. أنا dot-com. تحقق من أنني أنا dot-com. وجدتها! نعم، أنا كذلك! رائع. دعني أن أخبرك فقط أين يوجد bigbank. Bigbank موجود على الرقم 2.2.2.

شخص غير محدد: .2

شخص غير محدد: .2

شخص غير محدد: مرحبًا، bigbank. من فضلك هل بإمكانك أن تخبرني بمكان www.bigbank.com؟

شخص غير محدد: بالتأكيد. لكن، ليس لدي أي توقيع، لذا يتعين عليك أن ترفضني.

شخص غير محدد: آه، حسنًا! إلى اللقاء. مرحبًا، bigbank. من فضلك هل بإمكانك أن تخبرني بمكان www.bigbank.com؟

روس موندي: في حقيقة الأمر، يوجد مكان www.bigbank.com في 2.2.2.3.

تيم: شكرًا. هل بإمكاني التأكد من توقيعك؟

شخص غير محدد: رنين!

شخص غير محدد: www.bigbank.com توجد في 2.2.2.3 وهي موقعة.

تيم: ممتاز! يمكنك التفضل وايداع أموالي بأمان.

شخص غير محدد: المااااال!

ويس هارداكر: حسنًا. من فضلكم قدموا مساعدة في الإجراء النهائي بخصوص مجال التحرك في المرحلة الثالثة. أعرف أننا بحاجة إلى أمر فريد للتأكد من الأشياء عند ظهورها في المستقبل. سيكون ذلك رائعًا.

حسنًا. حسنا، أمر سخيف كهذا، هذا ما وقع بالفعل في جهاز DNS وأيضا مع DNSSEC. بالطبع، فالأمر أكثر تعقيداً شيئا ما من ذلك. لكن، في الواقع، يقوم المحللون فعليا بالربط الكامل وصولاً الى الجذور. فيقومون بتحليل مختلف أنواع TLD المقبلة والمستويات المتعددة للحصول على الجواب النهائي.

لكن، قد تكون هذه المستويات أحيانا عميقة، طالما أن الإمتدادات الأمنية لنظام اسم النطاق DNSSEC تحمي السلسلة بشكل تنازلي، وصولا إلى الحصول على جواب آمن، تماما كما يحمي الدخان الأزرق المحلل من التأكد من أن أوغ يرسل فعلا الرسالة الحقيقية.

لهذا، وعند هذه النقطة سأنقل الكلمة الآن إلى روس موندي. كان يجدر بي أن أعرف بنفسي أولا. حسنا، أنا ويس هيرداكر من معهد علوم المعلومات التابع لجامعة جنوب كاليفورنيا. روس موندي هو من بارسونز، وسيقوم بشرح أكثر لسبب حاجتكم لـ DNSSEC.

روس موندي: شكرًا لك، ويس. وأيضا شكرًا جزيلاً للفاعلين الآخرين الذين حضروا معنا اليوم. كان ذلك أمرا رائعا أن نقوم بالعملية مع مجموعة من أشخاص جدد كون ذلك كان إلقاء جديدا. شكرًا لكم جميعًا على حضوركم معنا هذه الجلسة. أقدّر ذلك ، مجددا.

حسنا، هذا هو الجانب المتعلق بـ DNSSEC الخاص بالجلسة العامة التي تهدف إلى مساعدة الناس على التفكير في الأسباب التي تجعل أي شخص، سواء كان المستخدم النهائي أو مزود خدمة الإنترنت ISP، أو مشغل الخادم الرسمي قد يرغب في القيام بالتحقق من DNSSEC، إضافة إلى مرور د.ايفل إلى الوسط، كون ذلك هو أساسا ما صممت DNSSEC لعده.

لذلك، عندما تفكر في ذلك، وعندما كنا نتحدث عن هذا الأمر في اختصاصات DNS، فإن DNS لا تقوم بإرجاع ونقل الأموال بين المستخدم والبنك. هناك تطبيقات في الحقيقة يتم استعمالها للقيام بذلك.

لذلك، عندما يهاجم الناس DNS والبيانات البديلة، ففي غالب الأحيان يحاولون القيام بذلك بسبب تطبيقات أخرى أو وظائف أخرى، والتي يتم القيام بها من خلال الإنترنت.

لذلك، في حال لا يشتغل DNS الخاص بك بشكل صحيح، عندها فلن يعمل أيضا سواء متصفح الإنترنت أو خادم البريد الالكتروني أو نوع من محرك المحادثة بشكل صحيح. لن تتمكن من فهم الأمور التي ترغب في فهمها أو المتوقع أن تفهمها.

لذلك، فهذا هو المشكل الأساسي من وراء رغبتك في الحصول على DNS بشكل صحيح: يتعلق الأمر بما يتعين أن يكون صحيحا، لذا فباقي التطبيقات التي تستغلها ستتمكن أيضا من الاشتغال بشكل صحيح.

إذن، فالمراد من العرض القصير هو التمكن من التركيز فعليا على جعل هذه المجموعات من التطبيقات البرمجية تتواصل مع جهات لا ينبغي للمستخدم كيفما كان أن يتواصل معها.

مع الوقت، أصبح هناك مجموعة من التطبيقات التي تمت مهاجمتها، مع هجوم يبدأ في DNS. في الحقيقة، بعض الهجومات التي تبدأ في DNS تنتهي بخلق نوع من الاستغلال لاثنين أو ثلاثة وأحيانا أربعة بروتوكولات أخرى للاستخدام. لكنها تبدأ بـDNS، وبالحصول على بيانات DNS على أن المرتكبين يرغبون في الوصول إلى هدف ما، حيث يتمكنون في الوصول إلى استغلال الناس.

لهذا، وفي نفس الوقت - أظن أن الأمر قد اختفى من الإنترنت، فلم أصادفه في بضع سنوات الماضية - وهناك خصوصا تكوين جامعي - في الحقيقة هناك تكوينان بجامعتين مختلفتين - بحيث يطلب من طلبة علوم الحاسوب الكتابة عن أداة الهجوم DNS. وهذا يعطي مثالا على مدى سهولة القيام بذلك نسبيا. وهناك برمجية متوفرة على الإنترنت وهي برمجية الهجوم DNS.

ولكن يكمن المشكل في الدروس الجامعية، على الأقل في البيانات على الإنترنت التي تتوفر عليها، في غياب أي جانب أخلاقي فيها وفي أن هذا الأمر لا ينبغي القيام به، وحتى الأستاذ يطلب منهم القيام بذلك كجزء من الدورات التكوينية.

لذلك، فليس واضحا ما مدى وجود برمجية القرصنة، لكنها موجودة، وسهلة الولوج وقابلة للكتابة، بالنسبة للأشخاص المهتمين بخلق البرمجيات.

لذلك، عندما يستغل المستخدمون DNSSEC، كما قال ويس سابقا وأشار إليه في عرضه، والفكرة هي التوفر على بيانات مشفرة ضمن الهيكلة العادية لـ DNS، لأن DNSSEC هي جزء من DNS. وهي مندمجة كليا مع DNS المعياري.

لذلك، عندما يتلقى مستقبل الجواب جوابا موقعا من DNSSEC، سواء كان التحقق على مستوى محلل التحقق المحلي، أو فعليا وبشكل مباشر على مستوى التطبيق نفسه، فالفكرة الأساسية هي أن المستخدم الذي أرسل استفسارا بشأن البيانات يمكنهم الحصول على تأكيد مشفر على أنه أتى من الجهة التي يفترض أن يأتي منها وأنه لم يطرأ عليه تغيير في طريقه.

لذلك، فما يتم القيام به فعليا هو أن تجعلك متيقنا، في الحقيقة من أن الأجوبة التي تحصل عليها هي البيانات التي ينبغي أن تستخدمها، سواء كنت تقوم باستفسار على الإنترنت أو كان ذلك محادثة خوادم البريد فيما بينها، أو كان ذلك جلسة جابر أو تويتر أو ما شابه ذلك.

لذلك، كمثال مبسط جار عن كيفية عمل تبادل DNS، يبين هذا المستخدم جو وهو يقوم باستفساره. لم أغير الأرقام كي تتلاءم مع ما تقوله قمصاننا قصيرة الأكمام. أعتذر على ذلك. على أي، يرسل جو استفسارا إلى ISP الخاص به، خادم الاسم المتكرر. يرسل بعدها خادم الاسم المتكرر استفسارا إلى خادم الاسم الرسمي للمكان الذي يريده المستخدم جو. يحصل على جواب من خادم الاسم الرسمي إلى خادم الاسم وبعدها يرجع ذلك الجواب إلى المستخدم جو. وكان هذا فعلا السيناريو الأول الذي رأيتم في العرض.

الشخص التالي بعد - آه، آسف. بعد رجوع الأجوبة تنساب البيانات بين التطبيقات نفسها. لذا، يقوم المستخدم جو بعدها بالحديث مع خادم الإنترنت ويقوم بنشاطه هناك.

الآن، عندما تتوفر على مجموعة من المناطق الموقعة لـ DNSSEC واشتغال وحدة حل التصديق، يمكنك تصميم المواقع الإلكترونية لتوفر مؤشرات، فعليا، على أن البيانات الصحيحة تم تبادلها. إلى حد الآن، فالأغلبية الساحقة من المواقع الإلكترونية التي قد تستعمل DNSSEC لا تتوفر على مؤشر مثل هذا، غير أن هذا أمر قمنا به منذ عدة سنوات خلت، حتى يكون بإمكان الناس رؤية جاهزية حصولهم على سلسلة DNSSEC في ذهابهم وإيابهم. إن كنت لا تتوفر على سلسلة DNSSEC تحته، تقوم بمؤشرات مختلفة عند رجوعها.

لذلك، فجزء من تصميم الموقع الإلكتروني هو دمج مؤشر الهجوم. وذلك الهجوم مشابه لـ د.ايفل، الذي يراقب عند ارسال استفسار ما. يسأل الخادم المتكرر الخادم الرسمي، ولكن قبل حتى أن يحصل الخادم الرسمي على ذلك الاستفسار، يمنح د. ايفل جوابا للمستخدم جو. لذلك، فإن المستخدم جو يذهب إلى المكان الخطأ. يذهب إلى موقع د. ايفل.

في غضون ذلك، فاستفسارات DNS المعيارية فإنها تقع على مستوى الشبكة، لكن آلة المستخدم جو عندها مسبقا الجواب، لذلك تتجاهل الجواب الصحيح وتبعث بالتطبيق للربط بموقع د ايفل.

لن يحصل أبدا على البيانات حتى تشتغل DNSSEC. عندما تشتغل DNSSEC، فإن المستخدم جو يرفض الأجوبة السيئة التي تراها في العرض وتذهب بعد ذلك إلى الموقع الصحيح.

تفضلوا.

الآن، وفي هذه الحالة، فالموقع الإلكتروني المجهز يتوفر على بيانات صحيحة، وبالرغم من قيامنا بذلك على الموقع الإلكتروني، قمنا بتجهيزه على نحو سيبين ذهابها إلى موقع إلكتروني آخر.

وهذا ما ستحصل عليه وحدة حل التصديق، ما ترونه بالعلامة الخضراء. وأول مدخل هو org.” يشارك Comcast DNSSEC، مشورة لـ “.ISPsلكن، وحدة حل عدم التصديق قد ترى أن ستيف كروكر قد يقول، DNSSEC” لا تحل مشكلة المجاعة في العالم، “كمدخل أول. وقد ترى أن الأمر التالي المنجز بالصفحة هو org.” يشارك Comcast DNSSEC، مشورة لـ ISPs.“

لذا، والأهم، هو كون البيانات تم ادخالها إلى الصفحة الالكترونية بشكل لا يمكن المستخدم، دون رؤية المثلث في الأعلى، على الإطلاق من أن تكون لديه فكرة على أن موقعه الإلكتروني يتعرض لهجوم قرصنة DNS، يقابله هجوم بديل المحتوى.

لذلك، يمكنكم القول أنه، ”ليس هناك الكثير من حلول DNS، هل هناك من حلول؟ “حسنا، حدث هذا قبل عشر سنوات عندما قمنا بقياس CNN. هذا قبل حوالي خمس سنوات. فمقابل صفحة محتوى واحدة من CNN.org، تطلب ذلك العديد من استفسارات DNS. لذا هناك الكثير من الاستفسارات.

والمعلومة المهمة حول DNS و DNSSEC - الجزء المهم - هو كون بيانات المنطقة نفسها هي ما يهم.

وتفسير آخر يبين كيفية اشتغال العملية والمكان الذي يحتاج إلى التغييرات. لذا، بإمكانكم أن تروا، على أقصى اليسار، أن بيانات المنطقة تم وضعها على مستوى الخدام الرسميين. وهي متوفرة إذن على DNS. لهذا، فالخدام المتكررون الذين ترونهم في الوسط يتواصلون مع الخدام الرسميين جوابا على الأسئلة التي يتلقونها من العميل.

لذا، فالزبون - كما يمكنكم رؤيته، .1، الصف الأول، الرقم واحد. الرقم اثنان، .المتكرر يسأل الرسمي. الرقم ثلاثة، الرسمي يجيب المتكرر. ومن ثم يجيب المتكرر على العميل.

لذا عند قيامكم بتنفيذ DNSSEC الخاص بكم، هناك خطوة تقومون بها وهي إضافة بيانات إضافية ووظائف إضافية. لذلك، في حالة التنفيذ في الجزء الخاص بكم لـ DNS، الذي تكونون

فيه إما مسؤولين على التشغيل أو التدبير - حسب موقعكم في المنظومة الشاملة لـ DNS للأمور ما يتعين عليكم القيام به، الأنشطة المرتبطة بشدة وعمق في DNS قد ترغب في القيام بهذه الإجراءات بنفسها لأن لديهم مسبقا فريقا مؤهلا لـ DNS.

لذلك في حال كان حجم وتعقيد ما تقومون به مرتبط بشكل محكم بـ DNS - فيمكنكم رؤية بعض الأمثلة هناك، [أرشيف]-السجل، شركة كبيرة، أنشطة بلا مناطق DNS مهمة التي تسهل إدارتها وصغيرة وسهلة التعامل - وهي من بين من قد يود القيام بهذا بنفسها، مجددا، لنتذكر أن حماية بيانات منطقة DNS نفسها تعد عاملا مهما.

لذلك، في التفسير الأخير، حيث ينبغي إضافة منطقة بيانات لجعل هذا وظيفة DNSSEC موقعة ومحققة - والبيانات الموقعة يضعها مالك الخادم الرسمي في الجهاز. وهي متوفرة إذن كي تضمن في الأجوبة. إذن، فالخادم المتكرر للتصديق التي يمكنكم رؤيته في الأسفل هو في الحقيقة من يقوم بالتصديق كي يقول، "نعم. هذا صحيح، بشكل مشفر."

لذلك، إن كانت المنظمة التي تتطلعون لها أو تعملون معها أو تتعاملون معها تمتلك العديد من أنشطة ووظائف DNS والعديد من مركزيات DNS، عندها يمكنكم ربما القيام داخليا بـ DNSSEC، يمكنكم القيام بذلك بأنفسكم.

إن كان للنشاط القليل من أو الاستخدام الأدنى لـ DNS بخصوص الوظيفة الرئيسية، فهناك احتمال كبير بوجود قسم تكنولوجيا المعلومات، أو ربما تم إسناد ذلك لمصادر خارجية بطريقة ما. يتعين عليك أن تسأل أحد المزودين، أكان ذلك قسم تكنولوجيا المعلومات أو المجهزون الخارجيون، إن كان باستطاعتهم القيام بـ DNSSEC. إن كانوا لا يستطيعون ذلك، قل "يتعين عليكم تعلم كيفية القيام بذلك، أو سأقول بنقل شركتي إلى مكان آخر، "لأنه في الحقيقة هناك عدد كاف من الأشخاص الآن في مشروع DNSSEC ما قد يصبح احتمالا حقيقيا. تستطيعون أن تختاروا الاستعانة بالمجهزين الذين تعتمدهم DNSSEC.

وهذه هي نهاية الجزء الرئيسي للعرض. نعتزم أن يكون هذا الأمر في إطار جلسة أسئلة وأجوبة مفتوحة جدا. سنفعل ذلك – أجل. سأرجع الأمر إلى ويس ليتكلف بتعيين الأشخاص، لأن معنا الكثير من فاعلي DNSSEC بالغرفة وأيضا أشخاصاً لهم دراية كبيرة حول DNSSEC.

لذا، من فضلكم اطرحوا أي سؤال. فنحن مستعدون بشكل كامل للتطرق إلى أي شيء تودون معرفته.

ويس هارداكر: حسنًا. لذلك، DNSSEC ليست بعد - .ماذا عن هذا؟ لا. أجل. أنا بحاجة إلى استرجاع الميكرفون.

تيست، تيست، تيست، تيست، تيست، تيست. حسنا - آه هيا لنبدأ. حسنًا. حسنًا. وهل يعمل هذا؟ حسنًا. إذن، لدينا اثنان. يمكنني استخدام الإثنين.

إذن DNSSEC ليست بهذه البساطة. وهناك تعقيدات كثيرة. نضمن أنه ستكون هناك أسئلة بالغرفة. إذن، في الحقيقة لدينا الكثير من الوقت لهذا الأمر مخصص فقط للإجابة على الأسئلة. لدينا العديد من الخبراء بالغرفة الذين ساعدوا في خلق DNSSEC، لذا وإلى حد كبير، إن كان لديكم سؤال، نستطيع الجواب عنه.

إذن، هل لدى أحد منكم أسئلة؟ ارفعوا أيديكم، وسوف نمدكم بالميكرفون.

ثانه نجوين: مرحبًا. أنا ثانه نجوين من فيتنام. شكرًا على هذا العرض التوضيحي. كان جد مفيد وتضمن العديد من البيانات [غير مسموع] DNS.

أرى أن العديد من [غير مسموع] من DNSSEC عند نشر [غير مسموع] لتأمين ccTLDs و gTLDs، غير أني أعتقد، في الحقيقة، أنه عندما تقومون بنشر هذا في DNSSEC، فأنتم بحاجة إلى التفكير في [غير مسموع] [لبعض المنافسين]. يبدو أنكم بحاجة إلى أن تكون لديكم [غير مسموع] توقيع DNS، DNSSEC، توقيع المنطقة، وبعض الخطوات نسيتها.

لكن، بناء على هذه الخطوة، أعتقد أن القراصنة أو [غير مسموع] يستطيعون الهجوم بواسطة الحجب المنتشر للخدمة DDoS، أو يستطيعون، بناء على ضعف DNSSEC، أن يصبحوا [مثل] وقت التزامن لـ DNSSEC، لأن الأمر يتطلب وقتا حتى يتم وضع الـ - قبل كل شيء، تضعون نقاطا إضافية لجهاز DNS، لكن يتطلب الأمر وقتا للانتظار قصد الحصول على الجواب. لذلك، يمكن لقرصان ما، بناء على هذا الضعف، مهاجمة الفجوة في جهاز DNSSEC.

لذا، هل لديكم أي حل لهذه المشكلة؟

ويس هارداكر: حسنا، أظن أنك سألت على مجموعة من الأمور. لذا، فأولها كان سؤالك حول إن كان لدى المستخدمين مهلة طويلة لطلب البيانات، صحيح؟ لأنه يتعين عليك طلب بيانات كثيرة، فهذا يبطئ نوعا ما بحث DNS. والأمر كذلك، نوعا ما، ليس ... المستخدمون الذين قد يكترثون أكثر هم الذين يستعملون تطبيقات فورية، حيث يحتاجون إلى القيام ببحوث DNS كثيرة ويحتاجون إلى النظر في جميع الأجوبة ومدى السرعة. لذلك، فهذا أساسا هو تصفح الويب وهذا النوع من النشاطات.

تذكر أنه وبسبب التخزين، أن هذا الأمر سيبطئ فقط بحثا واحدا والباقي منها، بما في ذلك سجلات السلامة، سيتم تخزينها.

لذا، فالبحث الأولي قد يكون في ترتيب أبطأ بالميلي ثانية، لكن بعده يتم تخزين ما وراء ذلك. لذا، أساسا، في حال رؤية المهلة، قد يراها فقط مستخدم واحد في ISP في وقت واحد، في طريقها إلى الموقع الإلكتروني.

أظن أن الأمر الآخر الذي سألت عنه هو كون بعض سجلات DNSSEC جد عريضة ويمكن استعمالها في تضخيم الهجوم.

لذا، إذا طرحت سؤالا على خادم DNS وقدم جوابا طويلا، وفي حال زورت مكان قدومك، عندها قد يذهب الجواب إلى الشخص الخطأ.

والحل الفعال لذلك هذه الأيام هو ما يطلق عليه محدودية نسبة الجواب التي تجعل معظم خدام DNS اليوم تمنعك من طلب العديد من السجلات واحدة. لذلك، في حال حاولت وطلبت بـ 100 سجل الكل في ظرف ثانية، فأنت لا تقوم بأمر صحيح وسأتوقف عن الجواب.

وبالتالي فهذا هو الحل الفعال اليوم. في الحقيقة أنا مسؤول مشغل لأحد خوادم الجذر. في اللحظة التي نشغلها، فجأة، نتلقى بشكل أقل الطلبات والأغراض كما يحدث. وكان هذا قبل سنوات. لذا، فهذا المشكل في الغالب لم يعد مطروحا.

أندرو، أظن أنه –

أندرو فريزر: أجل. هل يريد وارن أن يضيف شيئا إلى ذلك؟

وارن كوماري: لا.

أندرو فريزر: لا؟ حسنًا.

ويس هارداكر: حسنًا.

وارن كوماري: [غير مسموع] مهاجم يبعث جوابا لـ [غير مسموع].

ويس هارداكر: هل تريد المجيء والجلوس هنا، أيضا؟ أي خبير في الغرفة مرحب به للمجيء والجلوس إلى الطاولة حتى ...تفضل.

إيبيرهارد بلوتشير: مرحبًا. اسمي إيبيرهارد بلوتشير من ألمانيا. لست مختصاً. أنا شخص عادي تماما.

ويس هارداكر: حسنًا.

إيبير هارد بلوتشير: [غير مسموع]. لدي سؤال يرجع لفترة قديمة. أعرف أن DNSSEC موجودة منذ وقت طويل، أظن قبل عشر سنوات. شخص ما أخبرني أن ستيف كروكر بالتحديد هو من خلقها أو كان من بين الأشخاص الذين قاموا بذلك.

الآن، فهمت، بعد مرور الكثير من الوقت، أن لدينا الآن وضعا جديدا. هذه السنة، جميع عملائي النهائيين الذين أشرف لفائدتهم على خدمات النطاق يسألون عن تشفير SSL. لذا، لدينا Let's Encrypt وهي مجانية. لذا، أساسا، هذه طريقة أخرى، هذه السنة، لتأمين المواقع الإلكترونية.

فهمت أن شهادة SSL يجب أن تربط باسم نطاق واحد فقط، ما يعني أن السؤال هو، هل مازلنا بحاجة إلى DNSSEC أو ما هو الفرق بين DNSSEC و SSL للمواقع الإلكترونية المشفرة؟

في حال قمت بتشفير موقعي الإلكتروني مستعملا شهادة SSL، لماذا أزال في حاجة إلى DNSSEC؟

السؤال الثاني، ربما - اطلعت على الإحصائيات، وأعرف أن العديد من السجلات تزود البيانات بخصوص عدد النطاقات التي هي تشفير DNSSEC. وهناك بعض السجلات التي لها اختراق أدنى. لذا، فما السبب وراء ذلك؟ ومجددا، نفس السؤال: هل ما نزال بحاجة إلى DNSSEC؟

ويس هارداكر: سؤال رائع. لذا، من بين الأمور الأصعب بشأن أمن الإنترنت بشكل كامل هو أنه بإمكانك فقط حل مشكل واحد لأن جميع الأمور تعمل على شكل طبقات.

لذا، على سبيل المثال، إذا قمت ببحث DNS - لنقول أنك تتجه نحو موقع إلكتروني محمي SSL. لذا، تعرف أنك حصلت على موقع إلكتروني صحيح، في تمكنك من بلوغك هناك. ما أود قوله هو أن DNS يعمل قبل ذلك بكثير، وستوجهك فعليا إلى المكان الخطأ بشكل كامل.

هناك عدد من القضايا مرتبطة بذلك. أولها، يمكنها فقط أن تبعثك إلى المكان الخطأ ولن تحصل أبدا على الموقع الإلكتروني الصحيح. التوجيه له نفس المشكل. لذا، إذا لم نحم طبقة التوجيه والبنية التحتية للتوجيه - إذن، فالواقع أن الإنترنت مبني على حزمة. حقا، كل طبقة في تلك الحزمة بحاجة إلى الحماية قصد حماية المستخدمين النهائيين بشكل كامل.

لذا، نعم ما تزال هناك حاجة إلى DNSSEC.

هل ترغب في الحديث عن التاريخ والإنشاء وربما نشر DNSSEC وستيف كروكر؟ هناك العديد من الأشخاص الذين ذهبوا إلى DNSSEC. وقد ساعد ستيف بكل تأكيد، لكن ...

روس موندي: حسنًا، نعم. هناك تاريخ طويل للحصول على DNSSEC مصمم، منفذ، ومنشور. كما قلنا، فهي تهدف إلى التأكد من أن استخدام DNS الخاص بك يعطي جوابا مناسبا للمستخدم.

الآن، أي تطبيق يستفيد من ذلك فهو نسبيا [مستقل.] لذا، كان ذلك في الواقع سنة 1993، عندما بدأت جهود مهمة ومركزة للحصول على DNSSEC متطور ومصمم ومنظم. وكانت هناك اتصالات من هنا وهناك. ستيف كروكر كان من بين الأشخاص الذين شاركوا في إحدى هذه الاتصالات. كما أني من بين الأشخاص الذين قاموا بذلك أيضا.

لكن، كانت هناك عدة تصاميم مكررة وهذه هي المرة الأولى لدمج قدرة أمنية على الهواء في بروتوكول مشغل. كان هناك تصميمان لهما بعض المشاكل البارزة. والثالث حصل عليها بشكل صحيح.

في سنة 2010 تم التوقيع على منطقة الجذر نفسها. كانت هناك مجموعة من TLDs موقعة قبلها.

إذن، أجل هناك العديد من الأشخاص الذين قدموا العديد من المساهمات. هناك العديد من المنظمات التي عملت جديا على هذا. لكن، كان ذلك مركزا، وموجها، لمنع وقوع ما يوجد في هذه الشريحة لأنه، سواء كنت تستخدم شهادة SSL أو لا، هناك تحديات كافية مع سلطات الشهادة، وقضايا شهادات خاطئة أو سيئة، التي قد تواجهك، في الحقيقة، هذه النتيجة بالضبط تقع ولها إشكالية CA مرتبطة بالموقع الإلكتروني، وربما لايزال المستخدم يحصل على موقع إلكتروني موقع SSL.

ويس هارداكر: وأمر آخر يتعين تسجيله هو أن الإنترنت ليس الآلية التي يتعين حمايتها لأجل بحوث الاسم. البريد الإلكتروني مثال آخر جيد لا يمكن حله بواسطة نظام شهادة تقليدية.

لذا، سنتطرق إلى كل هذا يوم الأربعاء شيئا ما في ورشة DNSSEC، وهو أمر سنتحدث عنه لاحقا، والجميع مرحب به ليحضر. وسيكون برنامجا على طول اليوم، الكثير حول DNSSEC.

ومن بين الأمور التي سأتحدث عنها هي كيف أن DNSSEC هي الحل الوحيد المتوفر لحماية خدام الإنترنت من أن تمر على جهة في الوسط وأن تتم سرقة بريدك الإلكتروني والذهاب به إلى مكان خطأ. وشهادات TLS النموذجية لن تساعد في ذلك لسبب سأشرحه في ذلك اليوم. الأمر معقد.

لذا، أندرو؟

أحمد السادِه: اسمي أحمد السادِه. أنا زميل. سأسأل لماذا ليست منشورة على نطاق واسع، مثل DNS. لما لا ينشر الجميع DNSSEC؟ وهذا هو السؤال الأول.

وسؤال آخر هو، هل تعتقد أن التكنولوجيا الجديدة، مثل سلسلة الكتل، قد تكون حلا واعدا لحماية DNS؟ شكرًا.

ويس هارداكر: إذن الأمر مقسم إلى جزأين. لذا، الشخص الآخر سأل عن بيانات حول سبب كون بعض السجلات لها نشر أكبر وأمور مثل ذلك. هذا في الحقيقة سؤال جيد للغاية. كل جهة في العالم يبدو أن لها نسبة مختلفة للنشر وأمور مثل ذلك.

بعض TLDs تحديدا، السويد، جمهورية التشيك، وأخرى - تمنحك في الحقيقة حافزا ماليا لتوقيع منطقتك. لذا، فهي تمتلك حصصا كبيرة وأمورا مثل ذلك.

الكثير منها يأتي، هل هناك من حوافز؟ هل هناك تشجيع محلي لتشجيع الشركات فعليا لتستخدم هذه التكنولوجيا؟ إذن، نسبة التبني أصبحت بطيئة بشكل عام لغاية التشجيع.

لكن، نحن في الحقيقة بصدد معالجة الأمر - مرة أخرى، في حال أتيت يوم الأربعاء، فلدي إحصائيات رقمية، وقد أقف عندها - حسنا، يصعب القيام بذلك الآن. هناك الملايين من المناطق التي تم توقيعها الآن. لذا، حتى ولو كانت النسبة المئوية ضعيفة لأن هناك العديد من النطاقات،

فنحن بصدد الملايين والملايين من النشر. حوالي، 85% من TLDs تم توقيعها، أعتقد إلى حد الآن. لذا، فالأمر في تطور، لكن يلزم وقت طويل لجعل العالم بأكمله يتحول.

روس موندي: من بين الأسباب، إن كان بإمكاني إضافته إلى ذلك، ليس فقط TLDs والنطاقات في المستوى الثاني. فالمستخدمون النهائيون، أي المقاولات لم يطلبوا DNSSEC بكثافة لأنه في أغلب الأوقات لا يدركون مدى أهميته في أدائهم الوظيفي.

لكن، خلال الخمس السنوات الماضية، اتخذت الحكومة الأمريكية - تماشيا مع ما قامت به لخلق شروط توقيع جميع نطاقات gov. - وهو ما قامت به الحكومات الأخرى. لكن، الموقف الأمريكي هو الذي أعرفه جيدا.

كما أنهم يطالبون الآن بأن يتم التصديق لجميع نطاقاتهم. لذا، تم تشجيع الأمر للمقاولات النهائية في بعض المنظمات. على سبيل المثال، فالشركة التي أعمل فيها، بارسونز - parsons.com - هو نطاق موقع ويشتغل بتلك الطريقة.

لذا، فالأمر يبقي على التوعية، ويشجع الناس على السؤال. لهذا سترون العديد من الأمكنة تقول، "اسأل ISP الخاص بك، أو المزود أو أيا كان يقوم بخدمة DNS الخاص بك قصد تزويدك بقدرة DNSSEC."

ويس هارداكر: والعديد من أمناء السجل الجدد والسجلات تمتلك زرا للدفع. إن كنت ستقوم باستضافة DNS الخاص بك لديهم، فكل ما عليك القيام به هو النقر على الزر وستكون لديك منطقة موقعة. إذن، فالأمر جد بسيط.

لكن، بالنسبة للعديد من الأشخاص الذين يديرون DNS الخاص بهم، فهناك تكلفة مرتبطة بنشر أي آلية للأمن. لا يهم إن كان الأمر يتعلق بشهادة TLS أو DNSSEC أو أيا كان. عليكم معرفة ذلك. عليكم بالعمل على ذلك. هناك العديد من الأدوات الآن التي تجعل الأمر سهلا نوعا ما، لكن قبل عشر سنوات لم يكن الأمر كذلك. كان ذلك غريبا في ذلك الوقت.

هل من أسئلة أخرى؟ نعم؟

شخص غير محدد: مرحبًا. سؤالي يخص التعليق عن الاستبدال الأخير للمفتاح الأسبوع الماضي.

سؤالي الآخر هو، هل هناك من خطة لإضافة [متصفح التوقيع في DNSSEC]، إلى النطاق؟

ويس هارداكر: إذن، فمفتاح الاستبدال حدث الأسبوع الماضي، وهو الأول من نوعه. جرى الأمر بطريقة سلسة جدا. وهذا الأمر اتضح بشكل كبير.

هل تريد الحديث عن ذلك، يا جون؟

جون ليفين: هناك السؤال التالي.

ويس هارداكر: حسنًا. لديك السؤال التالي. إذن، فمفتاح الاستبدال تم فعليا بشكل جيد. لقد تأثرت بعض ISPs ولم تغير فعليا مفتاحها، لكن ليس متصفح الإنترنت من يحتاج إلى ذلك المفتاح. بل ISP، كما رأيتم مبكرا هذا اليوم. ليس في الحقيقة على مستخدم جو، بمتصفح انترنت، القيام بالكثير. ليس عليه حتى أن يعلم بوقوع DNSSEC.

وهناك قضايا أخرى شاملة تخص ما يحصل في حال تواجدك بمقهى بشبكة لاسلكية حيث يقوم ISP الخاص بك بـDNSSEC، فهل أنت محمي هناك؟ وهذا برنامج شامل مختلف آخر.

لكن، فقط ISP هو الذي يتعين أن يعرف المفاتيح الجديدة.

فيما يخص مستقبل ICANN بشأن، هل سيقومون بنشرها، وفي أي تاريخ، هذا سيكون محط نقاش، أظن لاحقا هذا الأسبوع، في الحقيقة. ربما خلال السنة المقبلة، سيكون هناك قرار بخصوص، إلى أي حد سنبقى نقوم بهذا الأمر؟ هل سنقوم بذلك بنفس الطريقة؟ ما هي آليتنا لنشر المفتاح؟

هناك الكثير من الأمور التي يتعين تحديدها بعد الدروس المستخلصة من هذا الحدث، لأنه كان ذلك فقط قبل أسبوع، أو أسبوع ونصف.

روس موندي: إن كان باستطاعتي، يا ويس، أمر آخر أود إضافته. ستكون بالطبع لدى المجتمع مدخلات بشأن أخذ القرار بشأن توقيت نشر المفتاح المقبل. هذا أمر تحرص المنظمة في ICANN - منظمة CTO - على الحصول على المدخلات من المجتمع. لذا، إن كانت لديكم مساهمات، أفكار، أو آراء، فهم يرغبون بكل تأكيد في سماعها. هناك آليات عديدة سيتم الاعتماد عليها للبحث عن ذلك، لكن فكروا في الأمر وساهموا بآرائكم.

ويس هارداكر: وسيكون هناك مجددا عرض بشأن نشر المفتاح يوم الأربعاء بورشة DNSSEC.

جون ليفين: مرحبا، ويس. اسمي جون ليفين. ساطرح نفس السؤال الذي أطرحه دائما، وهو، استضفت DNS لحوالي 300 منطقة لـ [غير مسموع]. بالنسبة لنصف هذه المناطق، فأنا البائع الوسيط لأمين السجل. لذا، فلدي ولوج مباشر إلى أمين السجل. بالنسبة لجميعها، فتوقيعات DNSSEC في الواقع تعمل.

بالنسبة للنصف الآخر، فأنا مزود الطرف الثالث DNS. مع أفضل [غير مسموع] في العالم، في هذه النقطة، بالنسبة لجميع المستخدمين الآخرين، فالشخص الوحيد الذي يستطيع أن يقوم بعمل DNSSEC هو المسجل، أو الشخص الذي يتوفر على بيانات الدخول الخاصة بالمسجل. لذا، إما أن أحرك مستخدمي ولو أن عملية تثبيت سجل DS، وهو أمر سهل بالنسبة لكم ولي ولكن ليس بالضرورة لأي شخص آخر، أو يتعين علي التوفر على بيانات الدخول الخاصة بحساب المسجل، الأمر الذي لا أرغب فيه.

أعرف أن هذا الأمر يمكن حله على مستوى أمين السجل بإضافة طريقة ما لتكون معلومات اتصال بمحين DNS، أو أمر يمكننا معالجته على مستوى IETF نوع بالتوفر على من - حسنا، كما تعلمون، نوع من أمر آلي.

لا يبدو أن أحد منها يحقق تقدما. خلصت إلى أني لست الحالة الأكثر شيوعا، لكن أعتقد أن مزودي DNS للطرف الثالث ليسوا نادرين، ويتعين علينا معالجة الأمر.

ويس هارداكر: أجل. وأنت محق بأن هناك عمل يتعين القيام به هناك، خاصة بالنسبة للأشخاص الذين يديرون الكثير من المناطق. قمت بجميع عملي يديويا لأني أخدم المناطق الخاصة بي كذلك. وهناك مجهود. الذي يتطور نحو الأفضل.

لذا، هناك بعض الأمور يمكنني إخباركم بها والتي تحققت في السنوات الماضية. أولها، هناك بعض المزودين الذي ينشؤون زرا في حال قمت بنشر سجل DS الخاص بك، تذهب فقط وتضغط على المفتاح الذي يقول، "هل هذا هو الصحيح؟ "لذا لا يتعين عليك القيام بعدها بلصقه. وسيذهب فعلا ليكتشف ذلك لك.

ثانيا، وارن كوماري - يجب عليك الحديث معه في وقت ما، أو [أوليفر]، الذي أنشأ سجل CDS، الذي يعد وسيلة لتحديث المفاتيح بشكل آلي للتواصل في DNS بين المنطقة الفرعية وأمين السجل.

لكن، أعرف –

جون ليفين: أجل، لكن لم تقم بتثبيتها. تقوم فقط بتحديثها عند هذه النقطة. [غير مسموع]

ويس هارداكر: هناك نقاش بشأن القيام بخطوة شجاعة للقبول وأمور مشابهة أيضا. تمت مناقشة هذا الأمر في الحقيقة كثيرا في الشهر الماضي: بدأ الناس - لماذا لا تأتي يا وارن؟ يتعين علي أن أدع وارن يتحدث عن هذا الأمر. لكن، الناس تتحدث الآن عن دفع ذلك أكثر إلى الإنتاج. لذا، سأبدأ أخيرا في رؤية حركة، لنقم بتنفيذ هذا. من قام بتنفيذ هذا؟ إذن، في الحقيقة، هذا ما حدث مؤخرا.

هل تريد أن تتحدث؟

شخص غير محدد: أجل.

ويس هارداكر: لندع وارن أولا.

وارن كوماري: كلا، أنت أولا.

شخص غير محدد: أجل. أود فقط التعليق على أن هناك على الأقل بلدين أو ثلاثة هذه الأيام حيث تعرف الآن (دفع سجلات CDS): الجمهورية التشيكية وسويسرا وليشتنشتاين. لذا، في تلك البلدان، إن كان لديك نطاق وقمت فقط بإظهار CDS في منطقتك، فسيأخذه السجل وبعده يتم إعداد السلسلة [بأكملها].

لذا، على الأقل هناك محاولات حيث بدأ هذا الأمر و، بالطبع، تبين أن ذلك سيكون مبادرة عالمية تدعمها dot-com. لكن، ربما هذه هي البداية وأمر يمكننا أن نتعلم منه. لذا، أعتقد أنه سيكون هناك عرض حول ذلك في ورشة DNSSEC هذا الأسبوع. لهذا، أدعوكم إلى الانضمام إلي ذلك. [غير مسموع].

ويس هارداكر: إذن، هناك عمل يتعين القيام به هناك، لكن الخبر السار هو وجود زخم إلى الأمام، أعتقد إلى غاية هذا الوقت. أجل، وهناك لجنة يوم الأربعاء، كما قلت.

رودولف دانييل: مرحبًا. طاب يومكم جميعًا. اسمي رودولف دانييل. وأنا زميل في ICANN.

ويس هارداكر: مرحبًا.

رودولف دانييل: لا أعلم إن كان الأمر ملائما، لكن استبدال KSK تمت الإشارة إليه للتو. أود فقط معرفة - الأمر حقق نجاحا إلى حد الآن، لكن هل تم مسح المفاتيح القديمة، أو لا زالت تشتغل؟

ويس هارداكر: إنه سؤال جيد. هناك أمران. حقق الأمر نجاحا إلى حد الآن. TTLs بشأن البيانات (Time To Live) المسموح لها أن تكون في الذاكرة المؤقتة كان ذلك فقط ليومين. لقد مرت الآن عشرة أيام؟ نسيت بالضبط. لذا، - أجل. يمكنني القيام بحساب ذلك. عشرة أيام. 21 ناقص 11. لذا، مرت عشرة أيام، ما يعني أنه لا يتعين أن تبقيه أي وحدة حل DNS لهذه المدة. يتعين عليهم أن يحينوا البيانات، وقد يسجلون فشلا، ما لم يقوموا بتشغيل أمر معطل للغاية.

لهذا، نحن تجاوزنا النقطة حيث - يتعين على أي شخص أن يسجل فشلا الآن.

في ما يخص إزالة المفتاح القديم، هناك جانبان في هذا الصدد. الأول، مازلنا نتوفر على المفتاح القديم بمنطقة الجذر، لكن لم يتم استعمالها. لازالت هناك، لكن لم يتم استعمالها.

في 11 كانون الثاني (يناير)، سيتم تمييزها. ستكون هناك علامة ستشير إلى، "حان الوقت الآن كي لا تثق فيها. "يطلق عليها صيغة الابطال. وبعبارة أخرى، فإنك تبطل ثقتك فيها. وسيتم نشر هذا لمدة ثلاثة أشهر أخرى، وفي 11 نيسان (أبريل)، سيتم حذفها فعليا من منطقة الجذر كليا.

لذا، فهناك الكثير بشأن عملية استبدال المفتاح. إلى حد الآن، ليس هناك توقع بأننا سنرجع إلى استخدام المفتاح القديم، لأنه يبدو أن الأمر عرف نجاحا.

حسنًا. إنه سؤال جيد. شكرًا.

شخص غير محدد: مرحبًا. هل هناك خطة لإدماج إشعار للمستخدم في المتصفح بشأن الشهادة، إن كنا [غير مسموع] الموقع مع DNSSEC؟

سؤال آخر. حسنا، سأقترح على عميلي استخدام ذلك com. وليس TLD العام لكونها غير موقعة في نطاقات المستوى الأعلى العامة. لذا، فهي تعد تسويقا أكثر بالنسبة للنطاقات الأخرى، ويتعين عليها الإسراع في تنفيذ DNSSEC.

سؤالي هو هل نتوفر على خطط لفائدة المستخدم لإظهار أن ذلك يشكل موقعا صحيحا؟

ويس هارداكر: آسف، ما كان السؤال الأخير؟ أي خطط لإظهار ماذا؟

شخص غير محدد: في المتصفح. [غير مسموع] حسنا، نستطيع أن نرى [غير مسموع] توقيع أي ... أرى في شريحة العرض في المتصفح، وأرى صورة في المتصفح. ربما هي مدمجة في امتداد المتصفح أو أمر مشابه؟

ويس هارداكر: هل تريد الحديث حول ذلك؟ لا؟ حسنًا. لذا، هناك في الحقيقة امتداد متصفح الذي تستطيع أن تتبثه يسمى DNSSEC ... أقوم بطمس الاسم. في حال قمت ببحث على امتداد المتصفح لكل من Chrome و Firefox، فهناك واحد يمكنك تثبيته والذي سيثبت في ICANN في المتصفح الخاص بك.

متعاقدو المتصفح ليسوا مهتمين جدا بالقيام بـ DNSSEC مباشرة في المتصفح بأنفسهم. وهذه قصة طويلة. يجب عليك أن تتواصل معهم وتقدم شكاية.

إذن نظام التحقق من DNSSEC - شكرا لك، تيم. نظام التحقق من DNSSEC هو اسمها. في حال حصولك عليها، فستقوم بتنصيبها. عندها عملت أنا وروس، قبل سنوات، على متصفح لم يشتغل بمكتبة DNSSEC الأساسية. يسمى المتصفح Bloodhound. لم يتم تحديثه، لأنه لا يتوفر على المفتاح الجديد، بالمناسبة. كان هناك استخدام واحد لذلك على [تويتر.]

روس موندي: أجل. يتعين التفكير في القيام بذلك.

ويس هارداكر: أجل. لذا، كان ذلك تغييرا لـ Firefox خصوصا للذهاب والقيام بـ DNSSEC مباشرة أسفل المتصفح. لذا، هناك استخدام أكثر يقع على مستوى البريد الإلكتروني وأغراض أخرى. مجددا، سأتحدث عن ذلك يوم الأربعاء، وسترون بعض مخططات اتجاه البريد الإلكتروني الذي يستعمل أكثر فأكثر مع [غير مسموع].

باري ليبا: بإخبار المستخدمين بذلك، هناك أدلة كثيرة مع الوقت على أن المستخدمين لا يفهمون ما سبق أن قلناه لهم، ومحاولة إخبار المستخدمين أن عدم معرفة معنى DNSSEC يعد أمرا لا يفهمونه فوق ما لم يحدث. والأمر دون جدوى.

ويس هارداكر: أجل. بعبارة أخرى، فالطريقة التي يتحدث بها الناس عن الأمر الآن هو إظهار رسالة خطأ دون تحديد القبول أو الرفض. لا تدعوهم يستمرون في ذلك. هناك أدلة كثيرة تقول أن المستخدمين النهائيين عموما لا يتوفرون على معرفة لاتخاذ قرار جيد للسلامة، لذا لا تدعوهم يتخذون قرار السلامة. قوموا فقط برفضهم.

وراءك أندرو.

شخص غير محدد: أجل، لكن فقط للتعليق على ذلك، فلا يعني أننا لسنا بحاجة إلى إشراك وإخبار المستخدم النهائي وأن نشرح له سبب ظهور تلك الرسالة. ولا يعني ذلك فرض حظر أو تجميد المحتوى. سيكون ذلك عبارة عن رسالة توضيحية، لأنه في حال كان ذلك المرة الأولى، حسنا، سيكون ذلك أمرا جديدا. فأنت لا تعرف ما هو ذلك الأمر. لكن، إن كانت الرسالة توضح نفسها بنفسها، على النحو الذي يجعل منها طريقة جيدة عندما تظهر في المرة المقبلة، فستساعد فعليا، أو ....

ويس هارداكر: أجل. هذا نقاش طويل وعام يخص الأمن حول طريقة السماح للمستخدمين بالقيام. أنا، شخصيا، باعتباري مهوسا فنيا، أتمنى أن يمنحوني اختيارا لرؤية أكبر قدر ممكن من التفاصيل. لكن، أعمل مع أقاربي الذين لا يدركون هذه الأمور، ويتصلون بي. لذا فالأمر يعد نطاقا كاملا.

هل لدى أي شخص آخر أي سؤال؟

شخص غير محدد: لديّ شخص واحد. لدينا العديد من القضايا. يمكننا التخزين في مضيف محلي، والمضيف [غير مسموع]. إن كنا نستطيع رؤية إشعار ما في المتصفح ... لا أعرف إن كان [غير مسموع] الوكيل، ويمكننا إحراز تقدم بشأن قضية أخرى للحصول على مزايا التوقيع. لذا، من الأهمية بمكان تحديد المستخدم وأن تكون العديد من القضايا [غير مسموع] للإنترنت.

ويس هارداكر: أجل. لذا، اليوم، فنحن نتحدث فقط على الأسماء. إذا كان الوكيل يستخدم أيضا وحدة الحل لـ ISP والتحقق، فستتم حمايتها كذلك. لكن، أنت محق فهناك العديد من الطبقات والعديد من وحدات التخزين المؤقتة في آليات صنف HTTP أو في البريد وجميع أصناف اللوازم الأخرى. جميع هذه البحوث لـ DNS بحاجة أن يتم التحقق منها للحصول على سلسلة أمن كاملة. أنت محق بشأن هذا الأمر.

شخص وراءك يا أندرو. خلفك دائما. هل رأيت ذلك؟

خوسيه ألبرتو: مرحبًا. اسمي خوسيه ألبرتو. أنا عضوفي برنامج الزمالة لـ ICANN.

سؤالي مرتبط بـ Tor. [عندما نستخدم Tor في أمر ما، فهل تنطبق سلامة DNS على Tor؟] يتم تطبيقه على، في هذه الحالة ... لا أعرف. هل هذا ممكن؟ أو، هل يستخدمون أمن آخر في DNS؟

ويس هارداكر: هذا سؤال جيد، والذي يذكرني في الحقيقة بأني تخطيت مبكرا سؤال سلسلة الكتل أيضا. هناك نظم تسمية بديلة مشغلة في الإنترنت. وهي أقل شهرة. و Tor إحداها. وهناك في الواقع Namecoin وهو نظام تسمية مستند على سلسلة الكتل. وهي غير متطابقة مع DNS. لذا، فـ

DNSSEC هي تحمي فقط DNS - حل التسمية المشترك. وهذا لا يمنع الآليات الأخرى من أن يتم استخدامها. ولا يمنعها من أن تتوفر على نظام حماية خاص بها.

لكن، كلا، لا أعتقد أن DNSSEC تنطبق على Tor. أفترض أنها، نظريا، تستطيع، لأنها تعمل مثل DNS. لست مختصا في To، لسوء الحظ. هل ثمة أحد آخر يريد التعليق؟

ليس كافيا للجواب عليه. حسنًا.

لذا، أظن أن لا هو الجواب الذي قد يساعد في هذا. غير أنه، يتعين عليك العمل مع شخص له دراية أفضل بـ Tor. لسوء الحظ، ليس معنا مختصين في Tor هنا بالغرفة.

لن ينجح الأمر. حسنًا. توصلنا إلى الجواب النهائي. لا، لن يساعد ذلك الأمر.

فان تشيه لين: مرحبًا. معكم فان تشيه لين من Chunghwa Telecom. أنا جايسون، بالمناسبة. إنه أنا مرة أخرى. حسب ما فهمت، DNSSEC مصممة لحماية تحويل DNS. قرأت مقالا يدعي فيه أن ملفات الارتباط لـ DNS يقدمها [RFCs, MTAs, MT3]. هل هناك طريقة خفيفة أكثر للقيام بذلك؟ هل تستطيع مشاطرة بعض الملاحظات بشأن ذلك المعطى؟

شكرًا. وأتمنى ألا أخرج كثيرا عن الموضوع.

ويس هارداكر: كلا،لا بأس بهذا. إذن، ملفات الارتباط لـ DNS تحل جملة من المشاكل. لذا، سأصحح الجملة الأولى التي قلتها. كونها تتضمن خطأ بسيطا. ليس الأمر سيئا، لكن قلت أنها تحمي التحويلات. DNSSEC لا تحمي التحويلات. بل تحمي البيانات.

حسنا، دعني أن أقدم لك مثالا. في حال أدليت ببعض بيانات DNS لروس وقلت، "خارج DNS، سأخبره بأن اسم مضيفي هو 1.1.1.1 وهذا هو توقيعي، "فيمكنه أن يعطي ذلك لجميع من يتواجد بالغرفة، حيث يمكنهم التحقق من كل ذلك. فهي تغلق في الواقع البيانات بنفسها.

ولا أكترث بطريقة نقلها. قد يكون ذلك عبر DNS. قد يكون ذلك عبر حمام الرسائل. لا يوجد فرق بينهما. ليس شبكة الاتصال هي التي تحميها DNSSEC. بل البيانات نفسها.

وهذا أمر مهم لكون التخزين المؤقت في DNS قد يتطلب أحيانا العديد من الوثبات. إن كنت تستخدم وحدة الحل 8.8.8.8 لـ Google، على سبيل المثال، لديهم عدة استضافات التي تتدارك النظام بذاكرة التخزين المؤقتة.

ولا يهم من يسأل ولا من يرد عليها. طالما أنك تستطيع التحقق من البيانات في النهاية، ولا يهم طريقة الحصول عليها.

وآلية ملفات الارتباط مصممة من أجل حماية تحويل واحد ضد، غالبا، الأمور الكبيرة جدا، وتسمح لك بالحصول على أجوبة كبيرة من الخادم، قصد منع وقوع نوع من الحجب للخدمة. قد يطلب الخادم منك التوفر على TCP أو شيء غير قابل للمقارنة.

لذلك، فملفات الارتباط تعالج مشكل مختلف. ولا تحمي البيانات داخل تحويل DNS.

شخص غير محدد: مرحبًا. حسب فهمي، لحماية بيانات DNS هناك آليتان للقيام بذلك. الأولى هي DNSSEC والثانية هي DNS عبر TLS [غير مسموع].

لذلك، أرى في الغالب أن DNSSEC هي المعروفة أكثر، المعروفة أكثر من DNS عبر TLS. إذن، هل يمكنك أن تقارن بين هاتين الآليتين؟ ما هي الميزة الأكثر ايجابية لـ DNSSEC بالمقارنة مع الأخرى؟ شكرًا.

ويس هارداكر: لديها أيضا هدفين مختلفين. DNSSEC، مرة أخرى، تحمي البيانات. لذلك، فلا يهم إن كانت عبر TLS أو لا. لا يهم كيفية حصولك عليها.

DNS عبر TLS مصممة لحماية التحويل بين شخص يطرح سؤالا والجهة التي يحصل منها على الجواب.

إن سأل متصفح الإنترنت الخاص بك ISP الخاص بك، فيمكنه القيام بذلك عبر الاتصال TLS للتأكد من أن لا أحد بالمقهى يطلع على طلبك. لكن، لا تعرف إن كانت وحدة الحل بـ ISP تستطيع أن تسأل الجذر و com و bigbank.com عبر TLS.

لذلك، DNSSEC تحمي السلامة، سواء حصلت على الجواب الصحيح أم لا. DNS عبر TLS مصممة لتوفير الخصوصية، للتأكد من لا أحد يرى ما تطلبه والأجوبة التي تحصل عليها.

يوما ما، قد يتم استخدام TLS في أي مكان، لكن لا تزال لا تعرف، بسبب كثرة الوثبات، في حال تم تأمين ما تحصل عليه من النقطة A إلى B إلى C إلى D. توفر DNSSEC الأمن بحيث تعرف أنها صحيحة بغض النظر عن عدد الوثبات.

كين هرمان: مرحبًا. طاب مساءكم. كين هرمان، مستشار مستقل. حسنا، أنا مقتنع بقيمة DNSSEC.

ويس هارداكر: مرحى!

كين هرمان: هل يمكنك أن تقول شيئا بخصوص مستوى الاختراق؟ كم عدد الأشخاص الذي يستخدمونها؟ كيف يمكن للمنظمات أو حتى الأفراد معرفة أن DNSSEC خلقت هذه السلسلة للثقة على طول الطريق؟

ثالثا، هل يمكنك أن تقول شيئا بخصوص تكلفة التنفيذ بالنسبة للمنظمات؟ قد لا تكلف الكثير بالنسبة للشركات الصغرى، التي تعتمد على ISPs الخاص بها، لكن قد يكلف ذلك الكثير بالنسبة للمنظمات الكبيرة. شكرًا.

ويس هارداكر: حسنا، عليك حضور ورشة DNSSEC. والعرض الأول لكل ورشة DNSSEC، التي ستكون يوم الأربعاء، هذه المرة - ستكون في وقت لاحق من الأسبوع خلافا للعادة - ستكون عبارة عن عدة خرائط وعدة بيانات حيث يقع الإختراق، وماهي الأجزاء التي تستعملها في العالم بكثرة، وأشياء مشابهة، بما في ذلك: سألقي عرضا عن عدد النطاقات [غير مسموع] والطريقة حسنا التي يتم بها نشر DANE. إذن، هناك الكثير من البيانات التقنية. لا أستطيع أن أكررها جميعها هناك. [غير مسموع] [البطارية] لذا يستسحن أن تحضر.

في ما يخص ... ماذا كان الجزء الثاني من السؤال؟

[كين هرمان]: الكلفة.

ويس هارداكر: حسنا، الكلفة. كان من الصعب القيام بذلك، إن سألت ISP الخاص بك ورجوته أن يشغل تحقق DNSSEC، فربما لن يقوم بذلك حتى يطالب الناس بذلك. وبعد أن يطلب العدد الكافي من الناس بذلك، يقومون بذلك. هذه الأيام، مسألة قلة الترتيب تحول دون تشغيلها، لذا ليس لديهم كليا الكثير من الأعذار، ما عدا حاجتهم إلى معرفة طريقة تنقيحها حدوث عطب. فهم بحاجة إلى معرفة ما الذي يحدث عند إدخال المفتاح.

أغلب ذلك يتعين أن يكون بشكل آلي هذه الأيام. في سابق الأيام، لم يكن الأمر كذلك، أنتم بحاجة إلى معرفة الكثير عن ذلك. وقد أصبح الأمر أكثر وضوحا الآن.

في الأيام التي تكون فيه القدرة فعليا على توقيع منطقتك، في حال ستقوم بذلك بنفسك - فستستضيف DNS الخاص بك، وستوقعه بنفسك - كان ذلك سلسلة من، مثل، أوامر 12. قمنا في الواقع بتوثيق ذلك في دليل نشر سابق. وكان ذلك طويلا وشاق للغاية. عملنا مجموعين أنا وروس. وقد توصل زملاؤنا إلى أداة واحدة. تشغل [اسم ملف-فضاء-الموقع-بالمنطقة] وسيتم ذلك، وتقوم بعدها بنشر النتائج.

لذلك، أصبحت الأدوات أكثر سهولة، وبذلك انخفضت الكلفة. لكن، ليس هناك أمر مجاني بخصوص الأمن. هناك دائما بعض الأمن.

وأمر آخر يتعين معرفته بشأن DNSSEC هو، إذا كنت ستقوم بذلك بنفسك، فـ DNS المستعمل من قبل ليقوم بـ نشر-و-انسى. ولم يكن عليك أبدا تغيير منطقتك. عليك فقط الخروج والنشر مرة واحدة. يمكنك أن تدعها لثلاث سنوات، و لاتزال البيانات في حال جيدة.

مع DNSSEC، لكونها مقيدة بالزمن، يجب عليك إعادة التسجيل مرة كل شهر، أو حسب الإعدادات التي اخترتها. كل شهر عادة. أعيد التسجيل كل أسبوعين بالنسبة لمنطقتي، حتى ولو كانت روابط الأمن جيدة بالنسبة للشهر.

شخص غير محدد: لدي ملاحظة واحدة على ما قلته للتو، لأنه، مع، على سبيل المثال، المحلل Knot، المشرف على التسجيل النهائي لمنطقتك ... إذا كان لديك نظام يقوم بنشر سجلات CDS، فهذا ما جرت به العادة بالضبط مسبقا. قم فقط بنشرها مرة واحدة، وستتولى جميع الآليات ذاتية التشغيل العناية بالأمن. لذلك، فالتكلفة منخفضة فعليا.

ويس هارداكر: أجل. لقد أثار نقطة مهمة. في حال أخبرت فقط المحلل الخاص بك - أظن أن معظم المحللين الرسميين يتوفرون على تسجيل آلي الآن - فسيقومون بتسجيلها لك. هناك العديد من الأمور التي تجعلها آلية بالكامل.

أنا مرتاب. أقوم بذلك على حاسوبي الشخصي، وكان ذلك بالأساس لكوني قمت بذلك من البداية، وليس لأنه لازال يتعين علي القيام بذلك.

هل من أسئلة أخرى؟ كان ذلك كله أسئلة رائعة. شكرًا جزيلاً لكم.

ثانه نجوين: حسنا، لدي سؤال آخر. ليس سؤالاً فنيًا. بالنسبة لبلد محدد كالفيتنام - لأني من الفيتنام - على سبيل المثال، في نظام DNS الخاص بحكومتي، فالأمر [غير مسموع]. نريد أن نغير جميع أنظمة DNS إلى DNSSEC. لذا، فما هي تكلفة التحول من DNS إلى DNSSEC وكم المدة؟ هل يمكنك تقدير المدة والكلفة؟

ويس هارداكر: هذا أمر يصعب تقديره، لذلك فأنا لست متأكدا ...

روس موندي: دعوني أدلي ببعض الملاحظات بخصوص ذلك. لن أعطي أي أجوبة دقيقة ومحددة لكن سأعطيكم فكرة.

لذلك، من بين الأمور التي حددها الناس عندما بدؤوا في القيام بـ DNSSEC والتمكن من إعداد وتشغيل الأمور أنه غالبا ما يجدون أن برمجية DNS الخاصة بهم لم يتم تحديثها على النحو الصحيح.

لذلك، فقد يكونوا يستعملون في الواقع، في محللي الاسم الرسميين، أو إن كانوا يشغلون أيضا ISPs ويقومون بمحللي الاسم المتكررة - التي قد تكون غير محينة لمدة ثلاثة، خمسة، أو حتى عشر سنوات. لهذا، فإن أول خطوة في مثل معظم هذه الحالات هو فحص حالة البنية التحتية لـ DNS الخاصة بك.

في حال كانت جيدة ومحينة والبرمجية حديثة، كما قلنا سابقا، فإن تحديات القيام بـ DNSSEC قد تكون أحيانا سهلة مثل القيام بتغيير إعدادات خيار أو خيارين في ملف الترتيب لأسطوانة التسجيل الأصلية الخفية التي تقوم بالتوزيع الفعلي خارجيا إلى المحللين الرسميين.

قد يكون الأمر جد معقد إذا أردت أن تقوم بإعداد آلية مشفرة مستقلة دون الاتصال بالإنترنت.

لذالك، فالأمر يختلف، لكن الأمر الأول والأكثر أهمية هو مراجعة البنية التحتية لـ DNS نفسها الخاصة بك. ابدأ من هناك. هناك الكثير من البيانات متوفرة على الإنترنت. ولطالما كان مجتمع DNSSEC مفيدا جدا في المشاركة مع الوقت، وهناك العديد من البيانات متوفرة على الإنترنت وتم ذلك حسب البلد.

ويس هارداكر: لذا، فـ ISOC تولت الموقع الإلكتروني الذي رأيتم في السابق، الذي كان نشر-DNSSEC، الذي يتضمن صورة ستيف كروكر. وهذا هو المكان الأفضل للبدء من أجل مصادر DNSSEC التي يمكن أن تساعد على طول المسار إلى غاية بلوغ الهدف. لذلك، فهذا موقع إلكتروني مهم يوفر الكثير من البيانات.

هناك آخر يسمى أدوات-DNSSEC وهو أكثر ذكاء شيئا ما. لكن، يمكنك التواصل مع أمين السجل الخاص بك أيضا. الكثير منها تتوفر على أدوات التي، في حال سمحت لهم باستضافة بياناتك ويشغلون خوادم DNS، أيضا، فيقومون بتسهيل الأمر للضغط على خانة الاختيار.

لذلك، فالتكلفة تعتمد على ما ترغب في القيام به. عليك القيام بالتقييم الذي قاله روس. قال بالبدء بما تقوم به الآن ثم معرفة تكلفة الأمر من هناك.

رودولف دانييل: مرحبًا. رودي، مجددا، زميل ICANN. أود فقط التذكير مرة أخرى الآن بأني رأيت شيئا يممى EDNSSEC. هل الأمر كذلك هناك؟

ويس هارداكر: حسنا، أظن أنك تخلط بين أمرين. EDNS دون SEC هي توسيع في آلية DNS لإضافة بيانات إضافية عندما تطلب بيانات.

في الحقيقة، هنا حيث تقول، "أريد القيام بـ DNSSEC. من فضلك زودني بجميع التوقيعات والأمور الأخرى. "لذلك، فهذه آلية لتوسيع داخل DNS الذي تحتاجه DNSSEC.

رودولف دانييل: أجل، حسنًا. شكرًا.

ويس هارداكر: أي أسئلة أخرى؟ باري؟

باري ليبا: حسنا، إن كانت لدي دقيقة، أود التطرق إلى السؤال السابق بشأن DNSSEC و HTTPS.

في البداية، لا تذهب عادة إلى الموقع الإكتروني بواسطة HTTPS. تذهب بواسطة HTTP وتحصل على إعادة التوجيه. مهاجم ما قد يتجنبك بإرسال إعادة التوجيه وأن يخدعك بألا تستعمل HTTPS. لذلك، لازلت تحتاج إلى التحقق هناك.

ثم، توصلنا إلى أمر أطلق عليه Strict Transport Security، حيث الموقع الإلكتروني، عندما تذهب إليه، يقول "استخدم HTTPs، وبالمناسبة، استخدم دائما HTTPS ولا تقبل أبدا

الاتصال بي دونها. "هذا يستخدم تقنية تسمى أولوية-الاستخدام-حسب-الثقة، على أساس أن المهاجم لن يتصدى للطلب الأول.

لتفادي ذلك، يضع المتصفحون الآن لائحة أمن نقل صارمة في المتصفح، حتى لا تحتاج للثقة عند الاستخدام الأول. لا تحاول أبدا الدخول إلى ذلك الموقع الإلكتروني.

لكن، بعدها ستتوصل بـ CA احتيالية والتي أشار إليها روس، حيث، إذا نظرت في المتصفح الخاص بك ورأيت عدد سلطات الجذر التي يثق بها المتصفح الخاص بك، ستجد المئات منها، تختلف من Verisign إلى بعض الشركات لم تسمع بها قط من التايوان.

إذا تمت تسوية أيا منها واقتنعت بإصدار شهادة لفائدة bigbank.com، عندها ستكون قد تمت التسوية.

لذا، لتفادي ذلك، لدينا شيء يسمى DANE، حيث ينشر البنك السجلات و DNS الخاصة به للقول، "هذه هي الشهادات التي أريدك أن تستخدمها. "هذا الأمر لتفادي ذلك المشكل، لكن خمنوا ما يطلبه DANE؟ DNSSEC لأنك ستحصل على الشهادات من DNS.

لذا، فالأمر كله مرتبط ويتماشى مع ما قاله ويس بشأن كل شيء يحتوي على طبقات. تحتاج إلى حماية كل قطعة على طول الطريق.

ويس هارداكر: والواقع هو أنه، إذا كان أول أمر يضعه المستخدم في مجال أي تطبيق، الإنترنت أو طريقة أخرى، هو اسم ما، يتم النظر في ذلك الاسم. لذلك، فهذه هي أول نقطة ضعف. لذا، فهناك طرق أخرى لتفادي جميع هذه الأنواع من المشاكل، ولها كلها قضايا. لكن، إذا قمتم بحماية DNS، فبعدها ستبدأ الكثير من المشاكل فعلا في الاختفاء.

وهذا لا يعني أنه لا يتعين عليكم استخدام HTTPS بعد ذلك. فهذا يحل مشاكل مختلفة.

هل من أسئلة أخرى أخيرة؟

أحمد السادِه: مرة أخرى، أنا أحمد السادِه، زميل في ICANN. حسنا، عندما أرى التصميم هناك، فيجب على الجميع في السلسلة أن يمتلك شهادة أو التحقق من التوقيع. إذا لم يتم نشر إحداها، فستفشل DNSSEC. هل هذا صحيح؟ هل فهمت الأمر؟

ويس هارداكر: إنهاء. لا يتعلق الأمر بفشلها، لكنك تعرف جيدا الآن أنك ستذهب إلى مكان ليس بـ DNSSEC موقع، لذا ستواصل العملية وفي غياب الثقة.

حسنا، هناك أجزاء من شجرة DNS وهي غير موقعة، ومتصفح الإنترنت الخاص بك سيواصل الاشتغال معها بشكل جيد، لكون DNSSEC سيقدم لك جوابا. ستقول، "حسنا، هنا. تحتاج إلى الذهاب إلى bigbank.com. وبالمناسبة، فهم لم ينشروا DNSSEC. ليس لديك أي خيار. عليك مواصلة الذهاب مستعينا بـ DNS العادي."

لذا، فهناك هذه الآلية للسقط، حيث ينزل المحلل من السلسلة، وفي الأخير تصل إلى نقطة تقول، "لا أستطيع القيام بالحماية متخطيا هذا، لكن ربما لا تزال ترغب في جواب على أي حال."

إذن، وصلنا إلى هذه النقطة اليوم، حيث هناك العديد من الأمور الموقعة وأخرى غير موقعة. لا نعطي الكثير عن رؤية المستخدم حيال ذلك، باستثناء رسالاتنا.

أحمد السادِه: حسنًا. شكرًا.

ويس هارداكر: حسنًا. ربما لدينا الوقت لسؤال آخر، إذا كان أي شخص يرغب في طرحه.

سؤال هناك.

شخص غير محدد: [غير مسموع]. هل تتوصل بالرسالة الخطأ في تلك الحالة؟

ويس هارداكر: إنه سؤال جيد. حسنا، السؤال هو، هل تتوصل بالرسالة الخطأ في تلك الحالة؟ أجل، لأنه ما يحدث - حسنا، لا تتوصل برسالة خطأ عندما تسقط في جزء غير مؤمن لأن ذلك هو فقط محللك يستمر في منحك الجواب. سيخبر محللك التطبيق الخاص بك إن كان قد توصل بجواب آمن أو جواب غير آمن.

الآن، فالمتصفحون أو التطبيقات الأخرى لا تنظر إلى بعض تلك البيانات لأن طريقة تقديم ذلك كما هو إلى المستخدم وما إذا كان ذلك خيارا سديدا تقديمه إلى المستخدم فهو امر معلق بخصوص ما إن كان سيفيد المستخدمين النهائيين أم لا.

ما ستتوصل به هو، في حال فشل DNSSEC في مرحلة ما، د. ايفل سيسارع ببعث رسالة حول عطب في الصفحة تقول، "لا يمكن ايجاد هذا الاسم، "لأن المحلل قام بالمحاولة. قام بمحاولة البحث عن الاسم، وفي حال لم يتوصل إلى جواب جيد لأنه يواصل الحصول على أجوبة سيئة ولم يتوصل أبدا بجواب جيد واحد، فستحصل على صفحة الويب التي تحصل عليها في حال ذهبت إلى أي اسم معطل. وستقول، "لايمكنني إيجاد ذلك الاسم."

لن تعرف أن ذلك كان بسبب DNSSEC التي تحميك. ستعرف فقط أنها فشلت في البحث عن الاسم لفائدتك.

حسنًا. إذن، وبذلك أعتقد أننا سوف ننهي جلستنا. هل لديك ملاحظات ختامية ترغب في إضافتها بخصوص يوم الأربعاء؟

روس موندي: حسنا، لدينا العديد منها ترويجية - غير مقصودة، لكنها دعاية - جيدة ليوم الأربعاء. سنعقد سلسلة من اللقاءات. إحداها ستكون بخصوص DANE. ستكون هناك فقرة تقديمية التي تتناول الخرائط التي تم خلقها التي اختارت كمية وطبيعة نشر DNSSEC بمختلف أطراف العالم، جغرافيا.

لذا ندعو الجميع إلى الرجوع يوم الأربعاء. ابتداءً من الساعة 9:00 إلى غاية الساعة 2:30 على ما أظن؟ كاثي، هل هذا صحيح؟

كاثي سكنيت: 03:00 ص.

روس موندي: 03:00 ص. حسنًا. لذلك، المرجو منكم التفكير في هذا الأمر. شكرًا للجميع على الحضور. بالتأكيد نتمنى أنكم تلقيتم أجوبة على الأسئلة التي طرحتموها. إن كنتم تودون التواصل مع أي منا هنا، أو أي من الفاعلين المتدخلين اليوم، بخصوص أسئلة DNSSEC، فنحن جميعا سعداء لمدكم بأجوبة إضافية وأن تكون لنا محادثات فردية بالبهو.

شكرًا للجميع.

ويس هارداكر: أجل. شكرًا. حسنا، نقطة واحدة أخيرة. بخصوص يوم التكنولوجيا، وهو يوم غد، تكون هناك عادة مفاهيم ونقاشات كثيرة ذات الصلة بـ DNSSEC التي تقع هنا، أيضا. وهي دائما ما تكون. لا أتذكر ما هو جدول الأعمال هذه المرة. لكن، غالبا ما تكون العديد من العروض حول TLDs التي تنشر DNSSEC وأمور مشابهة.

روس موندي: حسنًا. و يبدأ ذلك مباشرة بعد مراسم الافتتاح على الساعة 10:30.

ويس هارداكر: مباشرة بعد مراسم الافتتاح. حسنًا. شكرًا للجميع على الحضور. أتمنى أنكم استفدتم من هذا.

[نهاية النص المدون]