مونتريال - الامتدادات الأمنية لنظام أسماء النطاقات DNSSEC للجميع: دليل للمبتدئين
الأحد، الموافق 3 نوفمبر/تشرين الثاني 2019 - من الساعة 17:00 إلى الساعة 18:30 بالتوقيت الصيفي الشرقي
ICANN66 | مونتريال، كندا

دان يورك: أود أن أقول، ستكون لدينا بعض الأسئلة والأجوبة التي ستطرح في فترة وجيزة، وإذا كنت تريد أن تأتي أقرب قليلاً، فنحن في هذه القاعة الضخمة هنا اليوم، لذا يرجى عدم التردد في القدوم إلى هناك. سيكون لدينا ميكروفون، وسوف نتجول ونتحدث معك ونفعل ذلك.

أنا اسمي دان يورك، وأنا أعمل لدى جمعية الإنترنت المشاركة في بعض أعمال الدعوة الفنية التي نقوم بها هناك، وما نريد أن نتحدث عنه اليوم، ما هو DNSSEC، وما الغرض الذي يخدمه؟ وسوف نقوم بذلك من خلال عدة طرق. سنحكي لكم قصة صغيرة، وسنقوم بتمثيل مسرحية هزلية، مجموعة من القصص الهجائي، وسنتحدث قليلاً عن هذا، وسنحاول الحصول على القليل من المرح في هذه الأمسية اليوم الأحد.

بادئ ذي بدء، هل لي أن أطرح سؤالاً؟ كما منكم هنا قام بنشر واستخدام الامتدادات الأمنية لنظام أسماء النطاقات بطريقة ما؟ حسنًا، بضع أشخاص، أليس كذلك. حسنًا، كم شخص هنا ليست لديه أي فكرة عن ما تعنيه الامتدادات الأمنية لنظام أسماء النطاقات بالمرة؟ حسنًا، بضعة. أنا ألحظ التداخل مع الأشخاص الذين قاموا بنشر ذلك، فها نحن ذلك، نحن على ما يرام. إذن فسوف نعود بكم مرة أخرى ونخبركم بقصة أصول DNSSEC في عام 5,000 قبل الميلاد.

ومن ثم، كما تقول قصتنا، هذه هي أغوينا. وهي تعيش في كهف على جانب غراند كانيون وهذا هو أوغ، وهو يعيش في كهف على الجانب الآخر. والطريق طويلة بالنسبة لهم للعودة ذهابًا وإيابًا، وهكذا لا يمكنهم التحدث كثيرًا أو الزيارة أو أي شيء آخر كهذا. لذلك، في إحدى زياراتهم لاحظوا وجود دخان يخرج من نار أوغ. وهكذا، يدركون أنه يمكنهم الدردشة باستخدام إشارات الدخان؛ ويمكن أن يذهبوا ويرسلوا إشارات الدخان عبر ذلك، ومن الواضح أن بإمكانهم إخبار بعضهما البعض بمزيد من القصص، والتحدث عن ذلك، وإجراء محادثة أكثر من ذلك بكثير.

ولكن في يوم ما كان هناك رجل كهف آخر بالجوار وسوف نطلق عليه اسم كامينيسكي، ينتقل للعيش بجوار أوغ ويبدأ في إرسال إشارات الدخان الخاصة به. وفجأة، لا تتمكن أوغوينا على

الجانب الآخر من التفريق بينهما؛ فهي لا تعرف. "من يجب أن أكون...؟ ما الإشارات المناسبة التي يجب أن أراها هنا؟" إذن، تشرع في محاولة حل الأمر، "ماذا عسانا نفعل هنا؟ كيف يمكننا إنجاح الأمر بحيث أعرف أيهما هنا؟"

إذن يذهبوا من أجل استشارة كبار حكماء القرية. يظن رجل الكهف ديفي أنه قد تكون لديه فكرة. فينهض وينطلق إلى كهف أوغ ويذهب إلى الخلفية الأخيرة التي يرى فيها كومة من الرمال الزرقاء، ذلك الرمل الملون بشكل غريب، ولا يوجد إلا في كهف أوغ. فيأخذ بعضًا من ذلك، ويهرب ويقوم بإلقائه في النيران. فتتحول النيران إلى اللون الأزرق الرائع وفجأة، يمكن لكل من أوغوينا وأوغ التحدث، لأنها تعرف الآن أي الحديثين آت من أوغ. ولا يمكن لأحد آخر أن يتدخل، لأنهما يعرفان حقيقة أن الدخان الأزرق قادم من أوغ، وليس من شخص آخر.

وبطريقة مرحة، هذا هو كل ما يخص الامتدادات الأمنية لنظام أسماء النطاقات. فهي تخص التأكد من أنك تحصل على المعلومات الصحيحة من المرسل. وهي القيام بشيء خاص للمعلومات بحيث تكون لها القدرة على رؤية ماهية المعلومات الفريدة القادمة من ذلك الشخص. ومن ثم سوف نتحدث قليلاً ونتناول الأمر قليلاً من المنظور الفني.

وفي مستوى عالٍ، حسنًا، هذه هي الطريقة التي يتم بها في الغالب تصوير نظام أسماء النطاقات. وسوف نختم بالحديث حول جذر نظام أسماء النطاقات، ومعنا جميع هذه النطاقات من المستوى الأعلى، جميع نظام أسماء النطاقات الموجود، وجميع الأنواع والأشكال المختلفة. وبعد ذلك، معنا نطاقات المستوى الثاني دون ذلك. ومعنا كل هذه الموضوعات اليوم. وحدة تحويل نظام أسماء النطاقات إلى عنوان IP المقابل لها، وهو يعرف كيفية الوصول إلى الجذر، ويعرف كيف يخترق الترتيب الهرمي، وتعيين ومعرفة الأمر، وكل مستوى على طول الطريق يقوم بإخبار وحدة الحل قائلاً، "اذهب وتحدث إلى شخص آخر".

نظام أسماء النطاقات عبارة عن قاعدة بيانات موزعة. فهي تنطلق وتحاول حل كيفية الحصول على المعلومات من كل وحدة حل مختلفة، وتلتقطها على طول الطريق. لكن ليس هناك أي أمان في البروتوكول، كما في قصتنا القصيرة تلك، يمكن لأي شخص أن يتدخل وينتحل الشخصية، ويمكنه أن يقدم إجابات أخرى بطريقة مختلفة. ويمكنك تسميم الذاكرات المؤقتة لوحدات الحل تلك، لأنه بمجرد تخزين المعلومات، يمكن أن يتم احتجازها لفترة من الزمن.

ومن ثم سوف نقوم بتجسيد الأمر الآن. هل فرقتنا جاهزة؟ تفضلوا. سوف نوضح لكم قليلاً حول كيفية تجسد وتمثيل الأمر. إذن ما سترونه هنا هو أنه سيكون معنا هنا الشخصيات التي سوف تؤدي دور المستخدم، والذي سيرغب في الانتقال والبحث عن المعلومات، ويرغب في الاتصال بالموقع bigbank.com. إذن أثناء قيام فرقتنا بترتيب نفسها. حسنًا. انتظار. حسنًا. ها نحن ذا. حسنًا. إذن سوف يكون ويس هارديكر هو مستخدمنا، الذي سوف يتحدث إلى موفر خدمة الإنترنت، الذي يمثل وحدة حل اسم النطاق إلى عنوان بروتوكول الإنترنت الخاص به، وسوف تقوم وحدة الحل تلك بالتفاعل مع الترتيب الهرمي لنظام أسماء النطاقات المعاد ترتيبه هنا.

ويس هارداكر: اختبار واختبار، ثم اختبار.

فريد بيكر: المشكلة الأولى، أننا بحاجة إلى الكهرباء.

دان يورك: والصوت، هل يمكنكم إحضار هذا الميكروفون؟

ويس هارداكر: ها نحن ذا، اتفقنا.أعتقد أنني بحاجة إلى شراء يخت.دائمًا ما أردت شراء يخت.فهي عبارة عن قوارب كبيرة ورائعة وأنا أحب القوارب الكبيرة الرائعة.أعتقد أنني سوف أقوم بمراجعة البنك وأنا أقوم بأعمالي المصرفية في www.bigbank.com وسوف أستعلم عن مقدار ما لدي من أموال. هل يمكنكم التكرم بإعطائي عنوان www.bigbank.com بحيث يمكنني الانطلاق والتحدث إليهم؟

وارن كوماري: بالتأكيد، أنت من نوع العملاء الذين ينبغي الحفاظ على رضاهم.دعوني أبين ذلك لكم. مرحبًا أيها الجذر، أحد مستخدميّ يود الوصول إلى www.bigbank.com. هل يمكنك رجاءً أن تخبرني أين ذلك؟

فريد بيكر: حسنًا، أتمنى لو كنت أستطيع، لكن لدي مشكلة. أنا لا أعرف حقيقة. أنا لا أعرف أين أجد موقع .com.، ويمكنك أن تسأل .com.

وارن كوماري: حسنًا، شكرًا، سوف أجرب ذلك.مرحبًا .com. أحد مستخدمينا يود الانتقال إلى www.bigbank.com. هل يمكن أن تخبرني أين هو؟

متحدث لم يذكر اسمه: حسنًا، أنا لست متأكدًا من .www، لكنني أعرف bigbank.com وهو موجود هناك.

وارن كوماري: حسنًا، سوف أذهب وأسأله.مرحبًا، bigbank. مرحبًا، هل يمكن أن تخبرني أين www.bigbank.com تحديدًا؟

روس موندي: مرحبًا بك، مزود خدمة الإنترنت.يمكنني أخبرك أين هو www.bigbank.com فهو على الرقم 2.2.2.3.

وارن كوماري: على رسلك!لقد حصلت على إجابة أخيرًا. مرحبًا سيدي المستخدم، موقع www.bigbank.com موجود على 2.2.2.3، وهل يمكنني المجيء والتنزه على يختك في وقت لاحق؟

ويس هارداكر: أخشى أن يختي لا يسمح بوحدات حل متكررة وراجعة، لكن لا بأس. حسنًا، إذن يمكنني أن أتحقق من الأمر -- يا للعجب! لدي حمولة نقود تسع قاربًا.

دان يورك: هيا بنا نصفق لهم بحرارة على هذا الأداء. إذن هذه هي الطريقة التي يعمل بها نظام أسماء النطاقات. هذا ما يحدث طوال الوقت وجميع هذه الأرقام المهولة من استعلامات نظام أسماء النطاقات التي تجري. لكننا نود أن نتحدث أكثر حول الكيفية التي يؤدى بهذا ذلك. إذن فسوف نجري حديًا وحوارًا آخر. وسوف نقوم بهذا الأمر مرة أخرى، لكنكم سترون هذه المرة ما يحدث عندما يتورط مهاجم في الأمر.

ويس هارداكر: حسنًا، ها نحن ذا. اليوم هو اليوم الذي سأشتري فيه قاربي، يختي الكبير الرائع. أحتاج إلى الذهاب إلى bigbank.com مرة أخرى حتى أتمكن من تحويل أموالي، هل يمكن أن تخبرني أين هو مرة أخرى، لأنني نسيت؟

وارن كوماري: نعم، للأسف لقد نسيت أنا أيضًا.سأحل لك هذه المسألة رغم ذلك.مرحبًا، أيها الجذر.أحد مستخدمينا يود الانتقال إلى www.bigbank.com. هل يمكن أن تخبرني أين هو؟

فريد بيكر: أتمنى لو كنت أعرف الجواب. لكنني أعرف أين يوجد com. رغم ذلك. هل هذا مفيد؟

وارن كوماري: أجل، كذلك.نوع الجذر لا طائل منه، لذلك سوف أسأل com. مرحباً يا .com. أحد مستخدمينا يود الانتقال إلى www.bigbank.com. هل يمكنك أن تخبرني من فضلك أين هو؟

متحدث لم يذكر اسمه: حسنًا، ما زلت لا أعرف شيئًا عن .www، لكنني أعرف أن bigbank.com موجود على الرقم 2.2.2.2.

وارن كوماري: سأذهب وأطلب ذلك. مرحبًا...

أندرو ماكوناتشي: في الواقع، لا، لأن bigbank.com موجود على 6.6.6.6.

وارن كوماري: حسنًا، بالتأكيد. لا توجد أية مشاكل. مرحبًا سيدي المستخدم.

ويس هارداكر: أوه، 6.6.6.6، وأنا أعلم أين -- يمكنني التخلي عن كل أموالي لرقم 6.6.6.6، شكرًا لك. أين قاربي؟

أندرو ماكوناتشي: شكرًا. ها، ها، ها، ها، ها.

ويس هارداكر: قاربي؟

دان يورك: حسنًا. هيا بنا نمنحهم جولة أخرى. إذن هذه بالفعل هي طريقة عمل نظام أسماء النطاقات، وهو ما نتحدث حوله هنا جميعًا، يمكن العبث بنظام أسماء النطاقات بهذه الطريقة. يمكن للمهاجم القيام بذلك. بشكل أساسي، من يتمكن من إعادة الرد على وحدة الحل وتفسير رقم الموقع أولاً، هو الفائز. وكما تعلمون، فإن السرعة تفوز في هذا الصدد وإلى أبعد ما يمكن لأحدهم الذهاب والقيام بعملهم.

لذلك، في هذه الحالة، كان الدكتور إيفيل قادر على الدخول قبل أن يتمكن روس المكسين من الذهاب وإعطاء إجابة، والحصول على هذا الجواب هناك. الآن، ثمة جزء من الخطر أيضًا، ألا وهو أن وارن الذي يرتدي القبعة، وهو مزود خدمة الإنترنت لدينا، سوف يتمسك بهذه الإجابة لفترة من الزمن. إذن بالنسبة لأي شخص آخر يسأل عن مطان www.bigbank.com، فسيستمر في الحصول على الإجابة الخطأ...

أندرو ماكوناتشي: .6.6.6.6

دان يورك: بالضبط. سوف تكون هناك تلك الإجابة السيئة، باستمرار، إلى أن ينفد الوقت. هذه هي هجمات نظام أسماء النطاقات. وهي عمليات تسميم الذاكرة العشوائية والعبث بها. وكل هذه الأشياء موجودة بالفعل. ومن ثم فإن ما لدينا في الوقت الحالي، مرة أخرى، هو نظام أسماء النطاقات هذا. أما مع DNSSEC أي الامتدادات الأمنية لنظام أسماء النطاقات فيمكننا أن نضيف مفهوم التوقيعات الرقمية، ويمكننا أن نرى فرقتنا وهي لا تزال موجودة هناك، لأنهم سوف يقومون بتمثيل هذا المشهد مرة أخرى بعد قليل.

وما يحدث هو أن لديكم المفاتيح والتوقيعات التي يتم تخزينها في نظام أسماء النطاقات بحيث تكون لديكم القدرة على الفحص والتحقق، هل هذه المعلومات قادمة بالفعل من المصدر الأصلي؟ هل هذا بالفعل هو من يجب أن يقدم المعلومات حول bigbank.com؟ إذن فإن وحدة حل أرقام النطاقات، لكي ينجح كل ذلك، عبارة عن وحدة حل أرقام نطاقات تعلم أين يوجد مفتاح الجذر، أو تعلم كيف يمكن الحصول على ذلك. كما شخص سمع عن عملية تبديل مفتاح الجذر في العام الماضي؟ نعم، حسنًا. الناس ينظرون في هذه المسألة.

لقد كان هذا الأمر برمته يتعلق بالتأكد من أن هناك سلسلة ثقة من جذر نظام أسماء النطاقات، وصولاً إلى سلسلة من الأشخاص المختلفين، ومختلف الخوادم المعتمدة التي تقوم بتوفير هذه المعلومات. وجميعها مرتبطة ببعضها بحيث يمكننا حماية سلامة المعلومات الموجودة هناك. ومن ثم، فإننا نريد التأكد من أن خادم اسم هذا البنك الكبير، هنا تمامًا، أنه يمكن أن يكون هو من يقدم المعلومات إلى موفر خدمة الإنترنت، وليس لشخص آخر. إذن دعونا نستعين بفرقتنا مرة أخرى، بما أنهم هنا معنا، ولنقم بتمثيل وتجسيد الأمر مرة أخرى، وهذه المرة مع الامتدادات الأمنية لنظام أسماء النطاقات.

ويس هارداكر: سيسعدك أن تعلم أن هذه هي المرة الأخيرة.

متحدث لم يذكر اسمه: في البداية سوف نكون بحاجة إلى لافتات.

دان يورك: أوه. آه، نعم. يجب علينا استعراض هذا الأمر أولاً. تفضلوا أيها السادة. إذن، ما الذي نفعله هنا؟ الجذر يقوم بالتوقيع. والآن، ألا تفضل هيئة الإنترنت للأرقام المخصصة هذا إن كان سهلاً، اتفقنا؟ إذن، سوف تلاحظون أن الجذر قام بتوقيعها لهم، أي تم توقيع .com، وتم توقيع bigbank، وتم التوقيع للجميع. هذا جيد. والآن...

ويس هارداكر: حسنًا، لنتظاهر بعدم حدوث ذلك. لدي يخت آخر يستحق ثمنه ثروة من المال. سوف أقوم بشراء مركب آخر بالفعل هذه المرة. هل يمكنك أن تخبرني أين هو bigbank.com هذه المرة، وهل يمكنك الحصول على المعلومات الصحيحة؟

وارن كوماري: أجل، سأحاول.اسمحوا لي أن أنطلق وأسأل الجذر. مرحبًا، أيها الجذر، أحد المستخدمين لدي يريد معرفة مكان www.bigbank.com فهل لك أن تخبرني رجاءً؟

فريد بيكر: كلا، لا يمكنني ذلك. لكن يمكنني أن أخبرك أين تجد .com. وقد يكون .com قادرًا على إخبارك بذلك. وقد تم توقيعي.

وارن كوماري: اسمح لي أن أتحقق سريعًا من ذلك التوقيع.نعم، اتفقنا، هذا يبدو صالحًا بالنسبة لي.سوف أنطلق وأتحقق من .com. مرحبًا، .com، أحد المستخدمين لدي يريد شراء يخت. وهو بحاجة لمعرفة مكان www.bigbank.com. هل يمكنك أن تخبرني ذلك من فضلك؟

متحدث لم يذكر اسمه: لا زلت لا أعرف شيئًا حول .www، لكن يمكنني أن أخبرك بأن bigbank.com موجود على 2.2.2.2 وأنا يمكنني التوقيع على تلك الإجابة.

وارن كوماري: اسمح لي أن أتحقق من ذلك التوقيع. نعم، لا بأس بذلك، سوف أنطلق وأسأل عن ذلك. مرحبًا، www.bigbank.com.

أندرو ماكوناتشي: مرحباً.

وارن كوماري: مرحبًا، كيف حالك؟

أندرو ماكوناتشي: 6.6.6.6.

وارن كوماري: أين التوقيع؟ أنا لا أرى التوقيع [كلام جانبي] bigbank.com، هل يمكنك أن تخبرني رجاءً أن www.bigbank.com؟

روس موندي: حسنًا، يمكنني ذلك بالتأكيد www.bigbank.com. موجود في 2.2.2.3 كما أنه موقّع.

وارن كوماري: اسمح لي أن أتحقق من ذلك، وسوف أتحقق من ذلك بعناية. حسنًا، لا بأس بذلك إذن. ها نحن ذا، أيها المستخدم موقع www.bigbank.com هو 2.2.2.3 وقد قمت بتحقيق ذلك، ولك أن تثق في ذلك.

ويس هارداكر: نعم، شكرًا. سيدي البنك، هل يمكنك تحويل جميع أموال إلى دان يورك؟ أنا بصدد شراء قارب مستعمل منه.

دان يورك: لماذا، شكرًا لك، ويس. برجاء التصفيق الحار لهؤلاء السادة. إذن، هذه هي الطريقة التي نقوم بها بذلك وهذا كل ما يخص الامتدادات الأمنية لنظام أسماء النطاقات، ألا وهو الحصول على كل تلك التوقيعات التي تضمن أن شخصًا آخر لا يمكنه الدخول إلى تلك العملية.

وهذا هو ما تقوم به. وهذا هو كل ما تقوم به، وهو جزء هام. كل ما هنالك أنها تضمن سلامة وتكامل المعلومات، وأن ما تم وضعه في نظام أسماء النطاقات هو ما يحصل عليه المستخدم. والأمر لا يتعلق بالسرية، بل يتعلق بتأمين تلك المعلومات، ويتعلق الأمر وحسب بالتحقق من أن المعلومات هي ما قام المستخدم بوضعه تحديدًا. والآن للحديث قليلاً حول الأمر وضرب الأمثلة، فسوف نستعين بروس موندي، الذي سوف يأتي إلى هذه المنصة، وسوف أرد إلى ويس أمواله مرة أخرى.

روس موندي: شكرًا لك، دان. وشكرًا لكل من حضر للانضمام إلينا في فترة بعد الظهيرة هذه. سيدي، هذه الأضواء لامعة. إذن ما أريد الحديث حوله هنا، بشيء ما... آه، المطقطق، حسنًا. هذه هي أمثلة وأوصاف الأشياء التي يجب على الناس التفكير فيها وهم يستعرضون عملية نشر الامتدادات الأمنية لنظام أسماء النطاقات. هذا جزء من السؤال؛ "لماذا نقوم بهذا؟" وهو، "لماذا يعنينا شأن الامتدادات الأمنية لنظام أسماء النطاقات لكي نبدأ به؟" وقد تحدثنا بالفعل حوله من منظور نظام أسماء النطاقات وكيف أن معلومات نظام أسماء النطاقات يمكن العبث بها، ولا سيما إذا لم يكن لديك امتدادات DNSSEC مفعلة ونشطة.

ولكن لماذا يتابع الناس مسألة نظام أسماء النطاقات؟ فنظام أسماء النطاقات لا يستحق كل هذا الاهتمام. فعندما يسعى الناس من أجل القيام بأشياء لنظام أسماء النطاقات، فهي في جميع الحالات تقريبًا، إذن يمكنهم القيام بالأشياء بالنسبة للطلبات التي تنتقل فعليًا إلى إجراء استعلامات نظام أسماء النطاقات. إذن وكما رأيتم من قبل، عندما كانت لدى ويس رغبة في نقل الأموال، في تلك الحالة، فقد كانت محاولة من أجل سرقة الأموال. لذلك من المهمة بالنسبة

للطلبات، أن تستخدم نظام أسماء النطاقات، من أجل القيام بما تقوم به. إذن إذا لم تصل إلى المكان المناسب، فلا أحد يعرف ما سوف يحدث.

إذن فقد ضربنا العديد من الأمثلة، في العالم الواقعي بالنسبة لأشياء من هذا القبيل وكل -- بعض الأشياء تم تحديدها هناك في مجلس الإدارة وهي تخص أي تطبيق يتم تشغيله على الإنترنت اليوم. وهناك احتمالية كبيرة للغاية أن يتم استغلال نظام أسماء النطاقات تحت ثنايا ذلك، وفي غالب الأوقات لا يعرف مستخدمو التطبيقات وبصراحة لا يعنيهم وجود نظام أسماء النطاقات، لكنه من الضروري لكي تعمل تطبيقاتهم بالشكل الصحيح.

ومن بين الأشياء التي وجدتها منذ بضع سنين، وعدت وألقيت نظرة مرة أخرى، وللأسف لم أحتفظ بتفاصيل ما وجدته. لكن كان هناك أستاذ جامعي هناك وجدته في مسيرة أعمال البرمجة التي تطلبت من طلابه كتابة برنامج للسطو على نظام من أنظمة أسماء النطاقات.

وقمت باستعراض مجمل متطلبات وتصميمات الدورة التعليمية، ولم يكن هناك أي شيء يمكنني رؤيته تحدث حول الأخلاقيات أو أنه كان من الأشياء التي يتوجب عليهم عدم القيام بها. كل ما في الأمر هو؛ "مرحى أيها الطلاب. أنا أطالبكم بكتابة برنامج للسطو على نظام أسماء النطاقات"، وقد أصابني ذلك بالتشنج باعتباري شخص ظل يحاول منع عمليات السطو من الحدوث لزمن طويل.

ولحسن الحظ، لم أتمكن من العثور على ذلك لمدة خمسة أعوام مضت تقريبًا، فربما اختفي ذلك. إذن وكما قال دان، أن الأمر الأهم هو أن تكون لك القدرة على الوصول إلى المكان المناسب، وعندما تصل إلى المكان المناسب، أن تكون لك القدرة على التحقق من أن المعلومات التي تحصل عليها في المقابل صحيحة في حقيقة الأمر.

إذن فإن التشفير الأساسي العام المضمّن من أجل جعل الامتدادات الأمنية لنظام أسماء النطاقات تعمل في حقيقة الأمر هو الآلية الفنية التي تعمل في خلفية ذلك. والآن، عندما قمنا باستعراض بعض جهودنا السابقة، فقد قمنا في حقيقة الأمر في اجتماعات ICANN فعليًا بتشغيل برامج سطو برمجي حقيقية. هذه مجرد سلسلة من الشرائح التي توفر نفس الفكرة بشكل مصور مع ما رأيتموه في الأداء المسرحي هنا.

وأحد الأسباب وراء التوقف عن القيام بذلك على أرض الواقع، أنه في أحد الاجتماعات نجحنا في أن نقوم بدلاً من مجرد السطو على نظام أسماء النطاقات في القاعة الخاصة، حسنًا، لم يكن

تكوين الشبكة وفق المتوقع تمامًا، وقمنا بالسطو على نظام أسماء النطاقات لكامل اجتماع ICANN. وقد أثار هذا الأمر ضحك وسخرية الجميع عند انتهائه، لكنه لم يكن أثناء القيام بذلك. إذن فإن ما نقوم به هناك هو عرض الشرائح، ولكم أن تروا أن جو يوزر هناك في أسفل الركن الأيمن، ويريد أن ينتقل إلى خادم الويب الخاص به هناك.

ويمكنكم أن تروا، من خلال الصورة، أنه يرسل استعلامًا. وهذا الاستعلام هو الذي ينتقل إلى خادمه المتكرر. فيقوم الخادم المكرر بحفظه وإرساله إلى خادم الاسم الرسمي المرتبط بالويب. وخادم الويب الخاص به الذي يريد الانتقال إليه يحصل على إجابة مرة أخرى ويرسلها إلى الخادم المكرر. ثم يرسل الخادم المكرر مرة أخرى ويقوم بإخبار المستخدم. كان هذا ما رأيتموه، ونحن نتحرك جيئة وذهابًا، وندور بذلك حول المنصة.

والآن سوف نضع بعد ذلك، وبعد ذلك يمكنه في حقيقة الأمر إجراء المعاملة الخاصة به. إذن عندما نقوم بوضع مواقع ويب حقيقة، فهذا تكوين خاص بأحد مواقع الويب بحيث تكون الصورة المرئية على موقع الويب نفسه توضح إن كنت تقوم بعمل الامتدادات الأمنية لنظام أسماء النطاقات خلف الستار.

إذن ليست هناك أي صورة قياسية لتوضيح ما إن كانت هناك امتدادات DNSSEC، لكن الأمر كان من السهولة بمكان في إعداده ووضعه على موقع ويب بحيث يمكنكم رؤيته. وعندما تنتقلون لنفس موقع الويب، عندما لا تستخدمون آلية لتوثيق الامتدادات الأمنية لنظام أسماء النطاقات، فإنكم تحصلون على رمز مختلف. إذن، يمكنكم أن تروا أن ذلك الذي في الأعلى عبارة عن علامة اختيار وأن الموجود في الأسفل عبارة عن مثلث تحذير يقول لكم؛ "إن الامتدادات الأمنية لنظام أسماء النطاقات الخاصة بكم معطلة".

إذن عندما نقوم بنفس هذا النوع من الأشياء، أيضًا، فقد كنا نعرض على المنصة هنا أيضًا، أن جو يوزر يقوم بإرسال استعلام، لكن في هذه المرة فإن الدكتور إيفيل موجود على الشبكة. ومن ثم، ينطلق الاستعلام في البحث والتجول، وفي العالم الواقعي، فإن ما يحدث فعليًا هو أن الدكتور إيفيل يرى الاستعلام ويقدم إجابة، على الرغم من استمرار الاستعلام في التجوال عبر الشبكة، لكن يتم إرسال جو يوزر إلى موقع الويب المنتحل.

ويمكنكم أن تروا الاستعلامات الأخرى وقد اخترقت الشبكة وعادت مرة أخرى، وقدمت إجابة، لكن جو يوزر لم يحصل على تلك الإجابة، لأن وحدة حل العناوين التي كان يستخدمها تناولت

أول إجابة وذهبت إلى موقع الويب الخطأ، لذلك لم يتمكن من العودة إلى هناك ما لم يكن يستخدم الامتدادات الأمنية لنظام أسماء النطاقات. فعندما كان يستخدم الامتدادات الأمنية لنظام أسماء النطاقات فقد منعت الإجابة غير الصحيحة من الوصول إلى وحدة حل عناوين المواقع الخاصة به، وبعد ذلك وبعد أن حصل على الإجابة الصحيحة، عاد مرة أخرى إلى موقع الويب الصحيح وأجرى أعماله حسب المناسب.

لذلك، فقد صممنا موقعًا على الويب لإظهار ما يمكنك القيام به، وتحديدًا تم بناء موقع الويب حتى يتسنى لنا أن يكون هناك قسم من موقع الويب الذي تم عرضه، بحيث يكون مكانًا يمكن أن تحدث فيه اختطاف وسطو. ومن ثم فإن السطو الحقيقي الذي قمنا به ضد متصفح ويب لم يكن يقوم بأعمال الامتدادات الأمنية لنظام أسماء النطاقات، فقد قمنا في حقيقة الأمر بإدراج معلومات، والمعلومات التي قمنا بإدخالها كانت عبارة عن قصة زائفة تقول؛ "ستيف كروكر يقر بأن الامتدادات الأمنية لنظام أسماء النطاقات لن تحل مشكل الجوع في العالم".

إذن فقد كان هذا بشكل واضح والهدف منه في الإجمال أن يكون توضيحًا وشرحًا هزليًا، لكن إذا نظرنا في الصورة الأولي "نظام DNSSEC معطل" وللأسفل فسوف ترون أن موقع org. ينشر نصيحة الامتدادات الأمنية لنظام أسماء النطاقات من كومكاست لموفري خدمات الإنترنت، وبالنسبة لذلك المعروض في أعلى الصفحة، هذه هي القصة الأعلى. إن وبشكل أساسي، مع عملية السطو قمنا بإقحام جزء من المعلومات على صفحة، فحتى وإن كانت على نفس الصفحة في المتصفحات، كانت معلومات مختلفة وبالطبع تم إقحام معلومات زائفة.

ومن ثم، على صفحة ويب فردية، كم عدد، كما تعلمون، من خلال الانطلاق من خادم اسم فارغ دون معلومات مخزنة في الذاكرة المؤقتة، كما تعلمون. هذا هو موقع CNN.com منذ ما يقرب من ست أو سبع سنوات مضت ربما، وهناك ما يقرب من 75 إلى 100 استعلام ورد، فقط من أجل ملء صفحة واحدة. ومن ثم، يمكن السطو على أي من هذه الصفحات، أو على يمكن ذلك على قسم كبير منها.

والآن، هل تحسن الأمر قليلاً؟ لا، بشكل ما نعم، ولا في بعض الجوانب. هناك المزيد من الاستعلامات اللازمة من أجل ملء صفحة في موقع إلكتروني تجاري أكثر مما كان عليه الأمر في الماضي. لكن هذه الوثائق الخاصة توضح أنه يوجد في الوقت الحالي بعض من تلك الامتدادات الأمنية لنظام أسماء النطاقات موقعة، لكن العدد اللازم من أجل ملء أي موقع على الويب ربما تكون قد تضاعف في حوالي أربع أو خمس سنوات. إذن فإن الأمر الذي يهم الناس

في الكثير الغالب ويفكرون فيه كثيرًا عندما تتحدثون عن موضوع الامتدادات الأمنية لنظام أسماء النطاقات هو، "يا إلهي، هذه المفاتيح التشفيرية موجودة بالفعل. ماذا عسانا نفعل؟ من المهم جدًا الاهتمام والاعتناء بمفاتيح التشفير".

حسنًا، هذا صحيح، لكن الأهم من ذلك هو بيانات منطقة نظام أسماء النطاقات الخاصة بك. إذن، يتوجب عليكم إيلاء أكبر قدر من الاهتمام بدقة وصحة بيانات نظام أسماء النطاقات الخاصة بك بنفس درجة الاهتمام بمفاتيح التشفير، لأن المرحلة التي تحصل فيها على امتدادات أمنية لنظام أسماء النطاقات تكون مرتبطة بأي منطق، هي أن المستخدم الذي يحصل على تلك المعلومات يعرف أن معلومات نظام أسماء النطاقات صحيحة. ومن ثم، إذا ما أولينا مزيدًا من الاهتمام بمفاتيح التشفير الخاصة بك أكثر من اهتمامك ببيانات منطقتك، وكان هناك من يريد مهاجمة منطقتك، فسيهاجم ذلك الجزء في نظامك الذي يقوم بإدخال المعلومات في النظام.

وإذا ما قمت بتوقيع تلك المعلومات، فسوف يقول المستلم، "حسنًا، يجب أن تكون جيدة، فهي موقعة"، لكن إذا نجح شخص ما في الهجوم، ما يطلب عليه في الغالب اسم "جانب التوفير" في معلوماتك، بجزء نظام أسماء النطاقات الخاص بك، وحصل على المعلومات غير الدقيقة هنا، بطريقة ما، فإن وضعك أسوأ من الوقت الذي لم تكن تستخدم فيه الامتدادات الأمنية لنظام أسماء النطاقات، لأنك وبصفتك مشغلاً، تقوم بالتوثيق من خلال تشفير تكون فيه المعلومات صحيحة وإن لم تكن كذلك، فعليك مسئولية التعامل مع معلوماتك بشكل صحيح ومناسب.

إذن إليكم مثال آخر على القيام بأعمال نظام أسماء النطاقات دون الامتدادات الأمنية لنظام أسماء النطاقات. المنطقة، بالنسبة لبيانات المنطقة، في المكان الذي تضع فيه المعلومات على خادم الاسم الرسمي الخاص بك. إذن تدخل المعلومات، ويكون خادم الاسم الرسمي موجود على الإنترنت ويعمل ويحتوي على ذلك، ويتلقى طلبًا من خادم اسم مكرر، والذي تلقى أيضًا طلبًا من عميل فيقوم بالرد على ذلك الطلب.

لذلك، إذا كنت تقوم بإدراج نظام أسماء النطاقات في تشغيل نظامك، بدلاً من الاستعانة بمصادر خارجية أو توفير بعض السجلات لك، إذا كان نظام أسماء النطاقات مهمًا بما يكفي لوظائفك التي تقوم بتشغيلها وأنت تقوم بكل العملية داخل منظمتك الفعلية نفسها، من المحتمل أن يكون لديك أشخاص على دراية بنظام أسماء النطاقات DNS ضمن الموظفين. وربما ترغب في القيام بأنشطة الامتدادات الأمنية لنظام أسماء النطاقات كجزء فقط من ذلك، كتوسيع لما تقوم به، بإدارة نظام أسماء النطاقات.

إذن الأنشطة الكبيرة التي تجري في نظام أسماء النطاقات الخاص بهم، لا سيما حيث يكون نظام أسماء النطاقات حيوي على وجه الخصوص، فعلى الأرجح سوف يرغبون في تنفيذ الامتدادات الأمنية لنظام أسماء النطاقات الخاصة بهم وتشغيلها. ومن ثم، جانب ما من تشغيل نطاق المستوى الأعلى الكبير الذي تسجل من أجله، أو إذا كنت شركة كبيرة، وقد كانت hp.com مثالاً كبيرًا هنا، وشركة verisign.com، فأعمالها مرتبطة بنظام أسماء النطاقات، وهي من المؤسسات الهامة من منظور نظام أسماء النطاقات، ومن ثم سوف يقومون بإدارة الأنشطة الخاصة بهم.

وإذا كانت مناطق نظام أسماء النطاقات الخاصة بك هي من الأشياء التي قد لا تكون بنفس درجة الأهمية، سواء بالنسبة للإنترنت أو بالنسبة للجدوى الاقتصادية لمؤسستك. ومن ثم إن كنت، مثالي هنا هو أنه مثل net-snmp.org، ألا وهو النطاق الذي أعتقد أنني أملكه. وهو من النطاقات التي لا تقوم بأي شيء على الإطلاق. حسنًا، أنت تملكه الآن؟ حسنًا. لقد تنازلت عنه لويس. حسنًا.

لكن حقيقة الأمر أنه، أنها ليس عملية حيوية لنظام أسماء النطاقات بالنسبة -- من الجيد أن تكون على صواب، لكنها ليست حيوية بالنسبة للإنترنت، ولوظيفة الأعمال. وبعد ذلك، فإننا جميعًا نستخدم نظام أسماء النطاقات، ويجب أن نستغل الامتدادات الأمنية لنظام أسماء النطاقات متى ما أمكننا ذلك. ومرة أخرى، الشيء المهم هو حماية بيانات منطقة نظام أسماء النطاقات. والآن، فقد رأينا المثال السابق، حول تحميل المنطقة الرسمية وإجراء طلب للمعلومات والإجابة عنها.

ومن ثم، فإن هذا مجرد توضيح سهل ورائع على الأماكن التي تحتاج لمزيد من الخطوات. لقد حصلتم على توقيع البيانات للمنطقة الخاصة بكم قبل أن يتم تحميلها فعليًا في الخوادم المعتمدة لتلك المنطقة. الخادم التكراري أو التطبيق الطرفي، نتمنى ذلك في مرحلة زمنية ما، لكن الخوادم التكرارية نفسها بحاجة لأن يكون لها مفتاح جذر والقيام بعملية التوثيق، بحيث عندما يتم تقديم الطلبات ويتم الرجوع بالردود، يمكنكم في حقيقة الأمر القيام بعملية التوثيق نفسها. وأما بالنسبة لغالبية خوادم الاسم التي تقوم بالتوثيق، بالتأكيد المنتجات مفتوحة المصدر، فيمكن تشغيل ذلك من خلال ضبط مفتاح تكوين واحد فقط على الطريقة الصحيحة، هذا كل شيء، هذا كل ما يلزم للقيام بذلك.

والآن، وبإيجاز، فإن المفهوم العام للأنشطة التي تدير نظام أسماء النطاقات الخاص بها، فإن نظام أسماء النطاقات هام للغاية بالنسبة لهم. فسوف يتوجب عليهم القيام بأعمال الامتدادات

الأمنية لنظام أسماء النطاقات الخاصة بهم على طريقتهم، أي أنشطة DNSSEC الخاصة بهم، للتأكد من تشغيلها أيضًا بنفس مستوى دقة نظام أسماء النطاقات. وفي حالة وجود نشاط يستعين بخدمات تشغيل نظام أسماء النطاقات من الخارج، فربما يتوجب عليهم أيضًا الاستعانة بأنشطة DNSSEC من مصدر خارجي. وفي بعض الحالات، فإن هذا الأمر يزداد سهولة.

فالعديد من موفري خدمات نظام أسماء النطاقات الخارجيين لم يقدموا فيما سبق خدمات الامتدادات الأمنية لنظام أسماء النطاقات. ومن ثم فإنني أهيب بالأنشطة، إذا رأوا أن موفر الخدمات الذي يتعاملون معه، إذا ما استعنتم بذلك من مصادر خارجية، فلا تقوموا بأعمال DNSSEC بأنفسهم، بل اطلبوا منهم ذلك. وإذن لم يقوموا بذلك، فإنني -- فلن يقوم العديد من الناس بذلك، لكن العديد منا قام بذلك، وأنا معهم، فإن لم يعثروا على خادم يقوم بذلك ويقوم بتغيير من تدفعون له الأموال، من أجل تقديم خدمة نظام أسماء النطاقات، بحيث يقوم بأعمال الامتدادات الأمنية لنظام أسماء النطاقات.

إذن إليكم شريحة لتلخيص ما نقول. هذه هي المنظمات الراعية لهذا النشاط، هذا التجمع، ظهر هذا اليوم، تقدم مرة أخرى، دان. وفي بقية الوقت لدينا في حقيقة الأمر جلسة ومناقشات مفتوحة للأسئلة والأجوبة. وأرجوا منكم أيها السادة التقدم وسوف نتلقى بعض الأسئلة، أتمنى ذلك.

دان يورك: إذًا، نعم. وإذا كنتم أيها السادة تريدون المجيء والتقاط الميكروفون، فلدينا هذه التي من المفترض -- حسنًا، نعم، يجب أن تكون -- تقدموا. إذن من لديه أسئلة؟ لقد رأيتم ذلك كله. هل من أحد؟ تفضلوا، يجب على أحد القيام بذلك.

كاثي هنا، حسنًا، أندرو سوف يتجول حول الدكتور إيفيل. يجب أن يكون لدى أحدكم سؤالاً للدكتور إيفيل. حسنًا، هنا، حسنًا، شخص ما. كنت أخشى أن أبدأ في إلقاء النكات الأمر الذي يمكن أن يكون مؤلمًا. انظروا إلى وارن هنا. حسنًا، تفضل.

روكيو دي لا فوينتي: حسنًا، شكرًا جزيلاً لك على ذلك التقديم والعرض التوضيحي أيضًا. أنا روكيو دي لا فوينتي، وأنا زميل اجتماع ICANN66 وأريد فقط أن أستوضح إن كنت قد فهمت فهمًا صحيحًا، أن التوقيع الذي يلي بعد ذلك أنه من الأشياء الأساسية بالنسبة لنظام أسماء النطاقات، لذلك إذا لم

تقم نطاقات TLD بالتوقيع، فإن النطاق الذي أقوم بتسجيله لا يتوجب عليه ذلك أو أن هناك أي طريقة من أجل الحصول على الامتدادات الأمنية لنظام أسماء النطاقات بشكل صحيح؟

دان يورك: نعم. هل أي منكم يريد الرد...؟ إذن الإجابة هي، أعني، يمكنكم توقيع النطاق الخاص بكم، ويمكنكم القيام بكل تلك الأشياء هناك ولكنه لن يتم إدراجه في سلسلة الثقة لذلك فإن نطاق المستوى الأعلى، ومن ثم فإن شخصًا ما الذي يقوم بتوثيقه لن تكون له القدرة على تأكيد كل الأشياء وصولاً إلى الجذر الذي كان فيه. ومن ثم نعم، بشكل عام لكي يعمل نظام الامتدادات الأمنية لنظام أسماء النطاقات، يجب أن يتم توقيع نطاق المستوى الأعلى الخاص بك.

ويس هارداكر: ويتعين عليك حقًا توقيع كل شيء بشكل مثالي. إذن فإن نظام الامتدادات الأمنية لنظام أسماء النطاقات سوف يحميك من سقوط الجذر، طالما أن هناك شيء تم توقيعه. غالبية نطاقات TLD اليوم موقعة وأعتقد أنه سوف تكون هناك رسومات توضيحية في ورشة عمل DNSSEC سوف تقوم بعرض ذلك.

ثمة أكثر من 10 ملايين نطاق موقع، كما تعلمون، مثل النطاقات النهائية مثل bigbank.com، والذي قد يكون موجودًا بالفعل وربما لا يكون موقعًا. لكن يجب أن تكون لك القدرة على توثيق الشجرة بالكامل. وبهذا القول، وحتى وإن لم تتمكن من ذلك، حتى التوثيق وصولاً إلى com. هو أفضل من لا شيء إذا كان bigbank.com نفسه، إذا لم يكن هناك رابط أسفل من ذلك.

دان يورك: بالنسبة للنقطة التي أثارها ويس يوم الأربعاء، إذا حضرتم ورشة عمل DNSSEC، فسوف نحصل على مجموعة من المخططات التي توضح بعض الجوانب المختلفة الموجودة في ذلك الأمر، ونقدم أيضًا بعض الخرائط، وفي العديد من الأجزاء، لكنني لا أعلم أيها. من أي بلد أنت؟ الأرجنتين؟ حسنًا. أليست هي .ar؟ حسنًا، إنه يتحقق من الأمر. تفضل، هناك.

يزيد أكانوا: مرحبًا، أنا يزيد أكانوا، وأنا من دولة بنين، وزميل اجتماع ICANN66. أشكرك على العرض التقديمي وأقول أيضًا الفيلم السينمائي، فقد ساعدنا ذلك على الفهم تمامًا. لدي سؤالان، في الحقيقة. أولاً، ما السبب في نشر الامتدادات الأمنية لنظام أسماء النطاقات -- لا أعلم ما هي الكلمة الأنسب، لكن النشر والتوسع بطيء إلى حد ما. لماذا؟ هل هناك أسباب فنية؟ أسباب سياسية؟ السبب فقط؟

السؤال الثاني، لقد أخبروني عن برنامج العرض التعريفي بالامتدادات الأمنية لنظام أسماء النطاقات، هل تم نسيانه أم ماذا؟ ما هي الخطوة التالية في برنامج العرض العام لـ DNSSEC؟

وسؤالي الأخير، من أجل الحصول على مزيد من التوضيح حيال البنية التحتية اللازمة لاستخراج مفاتيح من أجل الامتدادات الأمنية لنظام أسماء النطاقات. فقد علمت أيضًا أن هناك بنية تحتية منفصلة يجب الحفاظ على سريتها أيضًا. هل لكم أن توضحوا الأمر قليلاً؟ شكرًا.

دان يورك: بالتأكيد. إذن تحديات عمليات النشر والتوسع، والعرض العام لـ DNSSEC، ومعلومات حول كيفية القيام بعملية التوقيع وما إلى ذلك، هل ذكرت ذلك بشكل صحيح؟ حسنًا. هل يريد أي شخص أن يرد على هذه الأسئلة؟ أو تناول مسألة واحدة منها؟

وارن كوماري: سوف أجيب عن بعضها. إذن فقد تحققت سريعًا من الأمر، ar. موقّع، إذن الأرجنتين... حسنًا، رائع. أما فيما يخص عملية النشر والتوسع، نعم، لم يتم نشر وتوسيع الامتدادات الأمنية لنظام أسماء النطاقات بما يكفي وبالسرعة التي كانت مفترضة. إلا أن بعض الإحصائيات المثيرة للاهتمام، فنحن في كندا في الوقت الحالي، وقد تم توثيق 13.3% من الطلبات داخل كندا، ونسبة 25% في الولايات المتحدة، ونسبة 19% في غرينلاند، ونسبة 14% في روسيا.

لذا، كما تعلمون، لا يتم نشرها على نطاق واسع، ولا يتم نشرها عالميًا، ولكن النشر يتزايد بالفعل، والأغلبية وليس الغالبية تمامًا، ولكن يتم التحقق من قدر كبير من الطلبات في الوقت الحالي، ويتم التحقق من أن الغالبية العظمى من نطاقات TLD تم توقيعها. ويشترط جزء من

عقود نطاقات gTLD الجديدة أن يتم توقيع نطاقات gTLD جميعًا وغالبية ومعظم نطاقات ccTLD يتم توقيعها أيضًا في هذه المرحلة.

دان يورك: تفّل يا روس.

ويس هارداكر: وإذا ما أردتم تعقب هذه الأشياء، بشكل يومي إلى حد ما أيها الزميل -- فيكتور، شكرًا لك، لقد كنت مترددًا في اسمه، فلدي أنا وهو موقع على الويب نقوم بتحديثه يوميًا ويطلق عليه اسم stats.dnssec-tools.org. ومن ثم فسوف يوضح لكم ذلك، وإذا ما ألقيتم نظرة على الرسم التوضيحي، ستجدون أن الأمر في نمو مستمر منذ 2011. وفي بعض الأحيان تكون هناك قفزات هائلة.

وقد كان هناك في الواقع، يوم واحد آخر فقط، لأن نطاق one.com وهو عبارة عن موفر خدمة، قام فجأة بتوقيع مجموعة من الأشياء تحت النطاق dk. لذلك كانت هناك تلك القفزات الكبيرة، وفي حقيقة الأمر من أجل تحقيق الانتشار والتوسع، فإننا بحاجة إلى المزيد من تلك الأشياء، نحن بحاجة إلى شركات عملاقة من أجل القيام بذلك افتراضيًا، لأن غالبية النطاقات الموجودة وقيد الاستخدام حاليًا في العالم لا تدار من خلال كل شخص فردي، بل تدار من خلال هذه الشركات التي تقوم بعملية استضافة نظام أسماء النطاقات.

ومن الناحية التقليدية، كانت هناك الكثير من القفزات الكبيرة، فالسويد بما أنها واحدة من الأوليات، وهناك أيضًا جمهورية التشيك، وقد كانت هناك محفزات عملاقة لدفع الناس إلى توقيع تلك النطاقات. المحفزات المالية، في حقيقة الأمر، من خلال جعل عملية التسجيل أرخص، دفعت في حقيقة الأمر بعملية التوقيع قدمًا ضمن أكواد دول خاصة. على سبيل المثال، من أجل المضي قدمًا.

دان يورك: روس، هل أردت المتابعة؟

روس موندي: نعم، أود فقط، ربما المتابعة فيما كان ويس يقوله للتو. وهناك الكثير من المحفزات المختلفة التي استخدمتها مختلف المؤسسات من أجل تشجيع الناس على إجراء الامتدادات الأمنية لنظام أسماء النطاقات. ومن بين الجوانب التي ساعدت كثيرًا هو أن غالبية وحدات حل أسماء نظام أسماء النطاقات المتاحة أمام الجماهير مما تشاهدونه الآن، بنفس الأرقام الأربعة، تعتبر شيئًا شائعًا إلى حد كبير. والغالبية منها الآن تقوم بعملية توثيق الامتدادات الأمنية لنظام أسماء النطاقات.

ومن بين الأشياء التي كان البعض منا يعمل عليها في هذه المساحة وقام بها على مدار فترة ليست بالقصيرة، هو أننا أردنا أن نرى التوثيق فعليًا ينتقل إلى التطبيق النهائي. كما أن المثال المشمول في هذا الملخص هو حيث أجرينا عملية السطو الإلكتروني التي ذكرها ستيف كروكر، "الامتدادات الأمنية لنظام أسماء النطاقات لن تحل مشكلة الجوع في العالم"، وأن عملية التوثيق نفسه تمت في المتصفح نفسه.

ومن ثم، وأنتم تنطلقون وتجرون الحوارات والمناقشات مع الناس، يجب أن تضعوا في اعتباركم أن توثيق معلومات نظام أسماء النطاقات الخاصة بكم تتم للمستخدم النهائي، كلما زاد مستوى الأمان الذي تحققونه في النظام نفسه. إذن يجب تشجيع الناس على التفكير في تجاوز ذلك، وحتى التخزين العشوائي الكبير لوحدات حل أسماء النطاقات العامة، والتفكير في القيام بذلك في التطبيقات. والآن، كان هناك سؤال آخر. أجل.

دان يورك: إذن اسمحوا لي في هذا الأمر الخاص أيضًا، فإن جزء من التحدي الموجود أمام النشر والتوسع هو أنه وكما توضح هذه الصورة، هناك جزأين في حقيقة الأمر، اتفقنا؟ كل من يقوم بالتوقيع ومن لديه نطاق بحاجة لتوقيعه. وهذا جانب واحد. ألا وهو الجانب الخاص بالتوقيع، حسنًا. والآن، البعض من ذلك وفقًا لما قاله روس، البعض من ذلك يمكن تحويله إلى نظام تلقائي؛ ولدينا الكثير من الأدوات المتاحة أمامنا. وإذا ما تحدثتم إلى أي من موفري خدمات نظام أسماء النطاقات الموجودين حاليًا، فيمكن للبعض منهم جعل هذا الأمر في منتهى السهولة.

وبعض الناس لديهم مربع اختيار، ففي ثانية، يقول لك لقد تم توقيع نطاقك. والبعض من هذا سهل، لكن الجزء الآخر في ذلك، الذي توجب عليكم فحصه، يجب عليكم القيام بتوثيقه. وكما

ذكر روس، في بعض الأحيان يكون الامر مجرد إلغاء التحديد أو إزالة سطر تعليق في ملف تكون، والآن، وعلى حين غرة، تكون لك القدرة على بدء التوثيق.

ولكن جزء مما حدث، وعلى مدار فترة طويلة، هو أننا عانينا من معضلة الدجاجة أم البيضة أولاً، كما يقال عندنا في الولايات المتحدة، من حيث -- بعض مشغلي الشبكات، أو موفري خدمات الإنترنت، مثل ما كان يقوله وارين، الذي يقوم بعملية توثيق الامتدادات الأمنية لنظام أسماء النطاقات، فقد كانوا يقولون، "لن نقوم بتشغيل عملية التوثيق لأنه لا يوجد ما يكفي من النطاقات الموقعة".

ومن ثم، فقد كان المشغلون يقولون، "حسنًا، لن نقوم بهذا الأمر لأنه لا يوجد ما يكفي من النطاقات الموقعة". وكان بعض كبار شركات توفير خدمات الاستضافة تقول، "لن نقوم بتوقيع النطاقات الخاصة بنا، لأنه لا يوجد ما يكفي من الأشخاص للقيام بالتوثيق". ومن ثم، كان هناك القليل من الأشخاص، كانوا يتوقفون ويقولون ذلك.

واليوم، تم التغلب على الكثير من ذلك، لأنه وكما قال ويس، هناك عمليات نشر وتوسعة حقيقة موجودة، وهناك عدد كبير من الناس ممن يقومون بعمليات حل أسماء النطاقات المتكررة. وإذا ما نظرنا إلى بعض خوادم نظام أسماء النطاقات العامة الكبيرة، فإن أشخاصًا مثل Google Public DNS وCloudflare وQuad Nine، والبعض منهم، فإنهم جميعًا يقومون بعملية توثيق نظام DNSSEC.

فإن كبار الشركات المختصة بحل أسماء النطاقات تقوم بذلك كبار شركات توفير خدمات الإنترنت تقوم بذلك، Comcast هنا في أمريكا الشمالية ولديها 20 مليون عميل ممن -- وهي تقوم بجميع ذلك من خلال توثيق الامتدادات الأمنية لنظام أسماء النطاقات. ومن ثم فإن هذا الجدل الذي تباطأ فيما يخص النشر والتعميم لفترة زمنية، تم التغلب عليه الآن، لكنه لا يزال مستمرًا. أنا أعلم أن لديك جزأين آخرين، فريد، هل أردت أن...؟ نعم، إنه مفتوح.

فريد بيكر: ومن ثم، فقد أردت أن أسأل روس سؤالاً. هل تعلم شيئًا عن برامج التصفح الخاصة التي تدعم توثيق الامتدادات الأمنية لنظام أسماء النطاقات؟ ما هو المتصفح -- لدي أربعة برامج تصفح فقط على جهاز الكمبيوتر المحمول. ما الذي يجب عليّ استخدامه؟

روس موندي: حسنًا، للأسف ليس هناك أي متصفح متاح يحتوي على توثيق الامتدادات الأمنية لنظام أسماء النطاقات مضمّن فيه. وارين، هل تعلم واحدًا؟ لقد كان لدينا واحدًا ويدعمه لفترة، لكنه لم يعد مدعومًا بعد الآن.

وارن كوماري: في حقيقة الأمر، انتظروا قليلاً. أعتقد أن ما تتحدثون عنه هو ما يقوم بتوثيق التحقق المستند على DNS للوحدات المسماة DANE.

دان يورك: لا.

وارن كوماري: إذن أعني جميع برامج التصفح، أي أن برامج التصفح تعتمد على وحدة حل للنظام. إذا كان جهاز الكمبيوتر الخاص بك يقوم بتوثيق الامتدادات الأمنية لنظام أسماء النطاقات. ووحدات الحل الموجودة في المتصفح تعتمد فقط وبشكل كبير على ما تقوم به وحدة الحل الخاصة بالنظام. ومن ثم، إذا ما قمتم بتمكين توثيق الامتدادات الأمنية لنظام أسماء النطاقات على أي وحدة حل يشير إليها جهاز الكمبيوتر، فسوف تحصلون على جزء من توثيق الامتدادات الأمنية لنظام أسماء النطاقات مجانًا. وأعتقد أن ويس سوف يحاول ذلك وسوف يصرخ في وجهي الآن.

ويس هارداكر: على الإطلاق. أنا لن أصرخ في وجهك أبدًا.

فريد بيكر: حسنًا. لقد أخبرتني للتو بصفتي مستخدمًا، أنني بحاجة على نظام ماك وعلى جهاز ويندوز وعلى جهاز لينكس، يجب عليّ القيام بشيء ما.

ويس هارداكر: إذن سوف نقوم بإخفاء ذلك باعتباره شيء فني للغاية أو من الصعب جدًا وصفه، ولكن هناك بعض العناصر التي يمكن أن تحدث فيها عملية التوثيق. ففي الوقت الحالي اليوم، فإن التطبيقات التي تحتوي على برامج لتصفح الويب وبرامج لقراءة البريد الإلكتروني وأي شيء آخر يقوم بالدخول إلى الشبكة، لا تقوم في العادة بعملية التوثيق بنفسها. كما في المسرحية الهزلية، منذ قليل، فإنني لم أقم - يلا سيد جو يوزر- فعليًا بالتحقق من تلك الشهادات بنفسي، فقد وثقت في موفر خدمة الإنترنت أن يقوم بذلك نيابة عني. وهي في حقيقة الأمر...

فريد بيكر: جو يوزر، أن شخص مزعج.

ويس هارداكر: أنا شخص مزعج. إذن فقد قمت بوضع كود توثيق داخل... في حقيقة الأمر، فإن حزمة طلب net-snmp، التي كان روس يتحدث حولها منذ قليل، فإن لدينا بالفعل كود توثيق في تلك الحزمة مفتوحة المصدر من أجل التحقق فعليًا منها في التطبيق. ولا يقوم بذلك إلا القليل جدًا من التطبيقات فعليًا. وهناك واحدة، تلك الواحدة من الكبريات، إذا ما ألقيتم نظرة على صفحة الإحصائيات التي كنت أتحدث حولها في السابق.

من بين أكبر المحفزات للناس على التوقيع والنشر والتوسع الآن هو أنها واحدة من بين -- هي في الواقع أفضل طريقة لتأمين البريد الإلكتروني بين الخوادم. ولذلك، في حقيقة الأمر، فإن هذا الأمر في تصاعد مستمر وسريع للغاية. وليس كل الامتدادات الأمنية لنظام أسماء النطاقات، لكن إذا ألقينا نظرة على ارتفاع وتيرة التحقق المستند على DNS للوحدات المسماة DANE، وهي عبارة عن تقنية تقوم بتوثيق محادثات البريد الإلكتروني بين الخوادم، وهذا في تزايد كبير وحقيقي، وهذا يتم على الأقل بالقرب من التطبيق، إن لم يكن فيه.

دان يورك: حسنًا، وارين. لديك...

وارن كوماري: فريد، لقد قلت بصفتك مستخدمًا، لقد سمعت بأنه يتوجب عليك القيام بشيء ما. بصفتك مستخدمًا، يجب عليك التأكد من أن وحدات الحل لدى موفر خدمة الإنترنت تقوم بعملية التوثيق، ولك أن تسألهم. أو استخدام واحدة من، كما تعلم، إن لم يكن لديهم، يمكنك اختيار واحد من وحدات الحل العام الكبرى، كما تعلمون، 111199998888، واحدة من تلك لأنها جميعًا للتوثيق.

وإذا أرت الحصول على حماية الامتدادات الأمنية لنظام أسماء النطاقات، فاستخدم واحدة من مزود خدمة الإنترنت إذا ما كانوا يقومون بعملية التوثيق، وإن لم يكونوا، فاستخدم واحدة من الأخريات. وهناك موقع على الويب، internet.nl، إذا ما قمت بالتصفح إلى ذلك، فإن به شيء سوف يتحقق فعليًا مما إذا كانت وحدات الحل المتكررة التي تستخدمها تجري عملية توثيق أم لا. ومن ثم، وبهذه الطريقة يمكنكم معرفة ما إن كان مزود خدمة الإنترنت يقوم بذلك أم لا.

دان يورك: أريد العودة مرة أخرى إلى سؤال يزيد، ولكن أيضًا، أود القول، فريد، إلى أبعد حد تصل إليه برامج تصفح الويب، الأمر الآخر وهو إذا كنا معرضين لإخفاء شيء ما، لكن اسمحوا لنا أن نترك الأمر حتى يوم الأربعاء. ولكن الأشياء التي بدأت في القيام بحل نظام اسم النطاق عبر بروتوكول نقل النص التشعبي الآمن، حيث تنظر برامج التصفح في ذلك، والقيام بكل تلك الأشياء، فإن الكثير من تلك المراحل النهائية التي تقوم بها، وهي خوادم DOH تقوم هي الأخرى بتوثيق الامتدادات الأمنية لنظام أسماء النطاقات. إذن قد يكون المتصفح فعليًا يقوم بذلك بحيث أنه إذا ما بدأ في المضي قدمًا في ذلك المسار، لكن اسمحوا لي ألا نخوض في موضوع DoH الآن.

اسمحوا لنا أن نعود إلى سؤال يزيد، لأنه كان واقفًا هناك بفارغ الصبر وأنا أعتذر إن نطقت اسمك نطقًا غير صحيح.

يزيد أكانوا: أنا اسمي يزيد. حسنًا، شكرًا. وشكرًا لك على توضيح مسألة توثيق وحدات الحل وتوقيع المنطقة، وهما أمران مختلفان، حسبما أفهم. فمنذ عامين، في بلادي بنين، اندهشنا عندما لاحظنا أن 80% من الامتدادات الأمنية لنظام أسماء النطاقات المطلوبة تم توثيقها من خلال

وحدات حل أسماء النطاقات. لماذا؟ لأن بعض مزودي خدمات الإنترنت كانوا يستخدمون وحدات حل عامة.

دان يورك: نعم.

يزيد أكانوا: وهذا الأمر مختلف تمامًا عن توقيع المنطق، وهذا هو سبب سؤالي. أين برامج عرض الامتدادات الأمنية لنظام أسماء النطاقات العام؟

دان يورك: نعم. إذن، وأنت على صواب مطلق، وهذا -- في نفس الإحصائيات، لا أدري، ويس، بالطبع، لكنني أعرف إحصائيات مركز معلومات شبكات آسيا والمحيط الهادئ المقدمة من جيف هوستون سوف توضح أن هناك بعض الدول التي لديها مستويات عالية للغاية من عملية توثيق الامتدادات الأمنية لنظام أسماء النطاقات جارية في الوقت الحالي. وعندما تقومون باستكشاف هذا الأمر، تجدون أن السبب في ذلك أن بعض موفري خدمات الإنترنت هؤلاء في بلدانهم، قد اختفوا ولا يستخدمون سوف خوادم نظام أسماء النطاقات العام فحسب. ولا يقومون بتشغيل وحدات الحل الخاصة بهم، بل يستخدمون 8.8.8، 1.1، 9.9، أو أيًا كان، واحد من وحدات الحل العامة المختلفة الموجودة حاليًا.

وإلى أبعد ما تصل إلى عملية العرض الترويجي لـ ICANN، فإنني لا أدري. سوف يتوجب علينا العودة مرة أخرى إليكم فيما يخص هذا الشأن لأنكم غير مشمولين في ذلك البرنامج المباشر. وسوف يتوجب علينا العودة مرة أخرى إليكم حول ذلك. إذن، يزيد، يجب أن تقدم لنا فقط واحدة، اسمك ويمكننا العودة إليك مرة أخرى حول ذلك.

وفيما يخص سؤال الوثائق حول ذلك، يمكنني أيضًا، يمكنكم العثور عليّ، هل يمكنني الحصول على رقمك؟ نشرت جمعية الإنترنت بعض المعلومات حول جانب النشر 360 الخاص بنا في موقعنا على الويب، وقد نشرت ICANN بعض المعلومات، وهناك عدد من الموارد المختلفة الموجودة والتي يمكن أن تتناول الموضوع بالتفصيل. والعديد من شركات الخوادم الرسمية،

ISC، وnlnet labs وبعضها الآخر، قامت باستعراض وإنشاء الوثائق الخاصة بها حول كيفية القيام بذلك. إذن هناك بعض الروابط الجيدة الموجودة حول ذلك. تعليقات أو أسئلة أخرى؟ نعم، السادة هناك.

متحدث لم يذكر اسمه: شكرًا. وتحت مخاطرة الحيود قليلاً عن الموضوع، فقد كنت أتساءل عن كيفية ارتباط الامتدادات الأمنية لنظام أسماء النطاقات بالرسومات التوضيحية، ردًا على ذلك.

ويس هارداكر: على الإطلاق، في حقيقة الأمر. فهي مختلفة. تم تصميم الامتدادات الأمنية لنظام أسماء النطاقات من أجل حماية مجموعة من البيانات وجعلها قابلة للتوثيق بحيث تفهمها بصرف النظر عن الطريقة التي وصلتك بها. القسم صفر وتوقيع التحويل TSIG عبارة عن تقنية أخرى داخل نظام أسماء النطاقات من أجل تأمين الأشياء، ولكنها في حقيقة الأمر تقوم بتأمين اتصال، وليس البيانات في حد ذاتها كما هي، بصرف النظر عن المسار الذي تتخذه. فهي تقنيات مختلفة.

دان يورك: نعم، تفضل.

وارن كوماري: وإلحاقًا بما قاله ويس للتو إلى حد ما حول هذا الأمر، فإن الامتدادات الأمنية لنظام أسماء النطاقات تتيح لكم توثيق المعلومات بصرف النظر عن الطريقة التي تصل بها إليك. ومن بين الأشياء التي تصل بنا من وراء كل ذلك، فإن عدد من الأشخاص يقومون في الوقت الحالي بتنزيل منطقة الجذر بالكامل في وحدة الحل الخاصة بهم، لأنها جميعًا موقّعة.

ومن ثم، يمكنكم فقط توثيقها داخل وحدة الحل الخاصة بكم ولا يتوجب عليكم إرسال استعلامات إلى الجذر. وهذا إلى حد ما من الأشياء الرائعة جراء الحصول على منطقة موقّعة، وهو أنه في بعض المواقف، يمكنك ألا تتعامل فقط مع الرد على الاستعلامات، بل يمكنك استيعاب ملف المنطقة بالكامل أو أن تدع شخصًا آخر يوم بذلك.

متحدث لم يذكر اسمه: هل يتعلق هذا بطلب التحويل والتنازل، أم أنك تحصل على ملف المنطقة بالكامل؟

وارن كوماري: العديد من حروف خادم الجذر، بما في ذلك الحرف ب-- الحرف ب والحرف و، ولا يمكنني أن أتذكر الحروف الأخرى، تتيح لك أن تقدم طلبًا بالتنازل والتحويل، آلية AXFR. فإذا ما كنت مهتمًا بالقيام بالمزيد من هذا، فهو يطلق عليه اسم الجذر المحلي وهو أحد الأسماء، ويسمى RFC 7706، وبه بعض المعلومات، وسوف يكون هناك إصدار جديد له قريبًا. لكن نعم، الجذر المحلي، أو الجذر المحلي الفائق --

دان يورك: الجذر المحلي الفائق، نعم.

وارن كوماري: -- به مشروع يتيح لك القيام بذلك من خلال صفحة ويب.

ويس هارداكر: حسنًا. الجذر الخاص بي في الواقع يطلق عليه اسم الجذر المحلي وهو localroot.isi.edu ويتيح لك التكوين الذي تحتاجه من أجل تحويل أي وحدة حل إلى وحدة حل التخزين المؤقت للجذر، بحيث يتم حفظ كل شيء مسبقًا في الذاكرة المؤقتة. وهناك الكثير من المعلومات حول ذلك، ونأمل أن يجعلها ذلك سهلة إلى حد ما بالنسبة لك، إذا كنت مسؤولاً واسع المعرفة؛ ربما ليس للمستخدم النهائي.

متحدث لم يذكر اسمه: وهل يمكنني فقط طرح سؤال آخر حول موضوع DNSSEC؟ إذا نظرت، على سبيل المثال إلى com.، فربما يكون لديها عشرات خوادم الأسماء. هل يحصل كل منهم على مفتاح DNSSEC فريد لكل مثيل أو جهاز فردي أم أنه واحد لنطاق TLD بأكمله؟

وارن كوماري: لذا، فأنت تقوم بالفعل بتوقيع منطقة، وبمجرد توقيع المنطقة، يمكن وضعها على أي خادم اسم. لذلك، يكون ذلك رائعًا بشكل خاص إذا كنت تدير خادم الاسم الخاص بك، ثم يكون لديك منظمة أخرى تكون تابعة بشكل ما أو تكون هي الخادم الثانوي. وقمت بتوقيع منطقتك، وتمنحهم المنطقة، ولا توجد مفاتيح أخرى مطلوبة. ومن الواضح، أنه ليس ثمة داعٍ للقلق من أن تصبح ضارة أو أي شيء.

دان يورك: نعم، هذا هو مكمن الجمال في هذه الطريقة التي تعمل بها، في هذا الصدد، لأنه بعد ذلك، كما قال وارن، بمجرد توقيعك على هذا النحو، يمكنك إيقافه في أي مكان. إنه مفتاح عام، أو مفتاح خاص، أي التشفير. تعليقات أو أسئلة أخرى؟ ويمكن أن تكون عامة، ويمكن أن تكون غبية، ويمكن أن -- لماذا تضم الامتدادات الأمنية لنظام أسماء النطاقات القسم SEC فقط أو شيء من هذا القبيل؟ لا أعلم. نعم، هناك في الخلف، يزيد.

يزيد أكانوا: سؤال آخر. أسمع أن هناك بعض التحريات، أو بعض التحليلات من أجل تغيير البروتوكول لاستخراج مفاتيح عامة وخاصة لمنطقة الجذر. أين تلك المناقشات وما هو التالي؟

دان يورك: حسنًا، أعتقد أن بعض الزملاء حول الطاولة يمكنه التحدث حول هذا، باختصار. أنت محق تمامًا. لذلك، في هذا التوقيع، عندما يكون لديك التوقيع، هناك على خادم التوقيع، فإنك تقوم بتسجيله باستخدام خوارزمية تشفير معينة، كما تعلمون. وعما إذا كان RSA أو ما إذا كان بنظام تشفير المنحنى الإهليلجي، وعدد من الأشياء المختلفة، ولكل من خوارزميات التشفير هذه خصائص مختلفة، بقدر كونها أكثر أمانًا، أو أكثر أو أقل صدعًا - كما تعلمون، بعض البروتوكولات الأصلية منذ ذلك الحين تم التغلب عليها بطرق مختلفة بحيث أصبح للناس القدرة على القيام بذلك.

وهكذا، تمت ترقية الأشخاص ليكونوا أكثر أمانًا. الآن نحن نبحث عن مفاتيح RSA سعة 2048 بت بطرق مختلفة. نحن نبحث في منحنى إهليلجي وهي أيضًا أصغر. نعم، هناك

خوارزميات مختلفة موجودة. بقدر حالة الجذر، وارن، يبدو أنك تريد الضغط على الزر الخاص بك. لا؟ حسنًا.

وارن كوماري: أعتقد أنني سأدلي ببعض التعليقات العامة.

دان يورك: لقد كنت تضغط على الزر هنا؛ كانت يدك عليه. إذن أعتقد...

وارن كوماري: لقد كنت أعبث بالزر. ها نحن ذا. لذلك، هناك الكثير من المعتقدات حول ما هو أفضل بروتوكول تشفير، وإذا وضعتم ثلاثة من معدي التشفير في غرفة، واحد منهم فقط سوف يخرج حيًا، لأنك طعنت الآخرين ودخلت في بعض الخلافات الضخمة حول، كما تعلمون، هل RSA أفضل، أم المنحنى الإهليلجي، أو ED 25519، أو أشياء أخرى مختلفة. في الوقت الحالي، كان هناك بعض الانتقال من RSA إلى بعض البروتوكولات الأحدث، ولكن أحد الأشياء التي بدأ بعض الناس يتحدثون عنها هو بروتوكولات الكم الآمنة.

هناك بعض القلق بين بعض مصممي التشفير من أن أجهزة الكمبيوتر الكمومية ستجعل الأشياء المشفرة الحالية غير فعالة. وهناك مجموعة من الأشخاص الآخرين الذين يعتقدون أن هذا القلق مبالغ فيه إلى حد كبير. ولكن هذا من الأشياء التي بدأ الناس ينظرون فيها، وقد تعلمون، في مرحلة ما، أنهم قد يبدأون في نشر بروتوكولات كمومية آمنة.

دان يورك: أعتقد أن الإجابة، أن تلك الموجودة في جانب الجذر، ليست هناك خطة فورية من أجل إجراء تغيير في البروتوكول. حسنًا، روس، هل تريد التغيير؟

روس موندي: حسنًا، لن نقوم بتغييره، لكنني أردت إجراء عرض ترويجي لورشة الأربعاء لدينا، مرة أخرى. أحد العناصر المدرجة في جدول الأعمال عبارة عن عرض تقديمي قدمه كيم ديفيس حول خطط العملية التالية لتبديل مفتاح توقيع شفرة الدخول الأساسية للجذر. لذلك، إذا كنت مهتمًا بمزيد من المعلومات حول تفاصيل متى وكيف تعرف كيف تناولوا جميع التعقيبات والآراء المختلفة، أي التي حصلوا عليها من المجتمع، فقد عقدت ورشة عمل DNSSEC بعد ظهر الأربعاء، على مدر 20 أو 25 دقيقة، حيث سيقوم كيم، الذي يرأس هيئة المُعرّفات الفنية العامة التي تدير هيئة الإنترنت للأرقام المخصصة، بتقديم عرض تقديمي حول مسودة الخطة التي تم إصدارها مؤخرًا، والتي أعتقد أنها صدرت يوم الجمعة أو السبت.

دان يورك: هذا خبر لم يسبق لأحد معرفته. بالمناسبة، ستكون ورشة العمل هذه في تمام الساعة 1:30 مساءً في القاعة المجاورة 517C، وتستغرق المناقشات عدة ساعات حول مختلف الأنواع حول DNSSEC، بجميع النكهات. البعض منها في مستوى عالٍ، والكثير منها به الكثير من المشكلات، والبعض في المنتصف، وجميع كل تلك الأشياء. ومن ثم، سوف تشهدون عددًا من يعود هناك ويقوم بذلك. تعليقات أو أسئلة أخرى؟

يقف أندرو هناك ويده في الهواء. يجب على شخص ما مساعدته. هل من أحد؟ هل من أحد؟ أمامك دقيقة من النصائح المجانية أو أيًا كان، وإلا، فسوف نطلب من وارن البدء في تقديم النكات مرة أخرى. هذا جيد. انظروا إلى هذا. ممتاز. فقط التهديد.

متحدث لم يذكر اسمه: حسنًا، قد يكون هذا سؤال بسيط بعض الشيء، لكني أردت فقط أن أوضح شيئًا ما في ذهني فيما يتعلق -- إنه في الواقع نوع من سؤال متابعة، طرحه فريد في وقت سابق. لذلك، وبشكل أساسي، إذا لم يكن لديّ متصفح يدعم DNSSEC، أو ما شابه Outlook أو أيًا كان، فهل يعني هذا أن القسم الموجود بين وحدة تحليل DNS الخاصة بي وأن عميلي غير محمي تقنيًا؟

دان يورك: نعم. والآن يجب أن نستوضح الأمر، كما كان يقول وارن أيضًا، جميع التطبيقات على جهازك من الناحية التاريخية دائمًا ما تركت حل DNS لجزء بسيط من الكود، أي وحدة الحل الجزئي

في نظام التشغيل، والذي انطلق وأجرى استعلامات إلى وحدة الحل الخاصة بموفر خدمة الإنترنت وللقيام بجميع تلك الأشياء التي كانت هناك.

ومن ثم، إذا لم يدعم نظام التشغيل الخاص بك توثيق امتدادات DNSSEC، والتحقق من التوقيعات، فنعم، فإنك معرض لخطر انقضاض الدكتور إيفيل وتزويدك بمعلومات زائفة يمكن أن تعيد توجيهك إلى موقع آخر. ومن الناحية التاريخية، كانت هذه هي الطريقة القديمة، من بين أشياء أخرى، مثل الأمثلة التي تراكم فياها الناس، كما تعلمون، توثيق DNSSEC داخل برامج تصفح خاصة، والأغلب لأغراض الاختبار.

وهذا الأمر يتغير إلى حد ما. فهناك مجموعة كاملة داخل فريق عمل هندسة الإنترنت، ITF، تنظر في حقيقة أن الكثير من التطبيقات تقوم بأعمال DNSSEC. بعض الأشياء الأعلى أهمية التي نسمعها حول DoH وبرامج تصفح الويب جزء من ذلك، لكن هناك تطبيقات أخرى تتعلق أكثر بتوثيق نظام أسماء النطاقات وأشياء بالطرق التي تغير بشكل ما من الطريقة والمنهجية التي يعمل بها نظام أسماء النطاقات والطريقة التي تعمل بها الإنترنت بطريقة ما. وراين ينظر إليّ وكأنه يريد أن يقول شيئًا ما.

وارن كوماري: أجل. يعتقد وارن أنك قد تكون في الواقع، أو ربما نحن جميعًا، قد أفرطنا في مدح الحماية هنا. لذا، ماذا يحدث بالفعل، إذا رأيت ذلك في المسرحية الهزلية، فقد توقف مزود خدمة الإنترنت وقام بجميع عمليات التحقق وعاد مزود خدمة الإنترنت في النهاية إلى المستخدم وقال: "لقد قمت بالتحقق من ذلك. لا تقلق، إنه على ما يرام".

فالطريقة التي يعمل بها نظام امتدادات DNSSEC في حقيقة الأمر، أن وحدة حل التصديق أو مزود خدمة الإنترنت أو نظام أسماء النطاقات العام أو أيًا كان، يقوم بعملية التوثيق وبعد ذلك يخبر العميل أنه قام بذلك وأنه يجب أن يثق فيه. وبشكل أساسي، فإنه يقول بشكل ما، "نعم، هذا رائع"، والكل سعيد. إذن فهذا يعني أنه إذا تم العبث بالحزمة في طريق عودتها من وحدة الحل إلى عميلك، فربما يكون هناك من يقوم بأشياء سيئة.

وفي النهاية، سوف يكون من الرائع لو أن الكمبيوتر الخاص بك قام بالتوثيق بنفسه، إذا لم يثق في مزود خدمة الإنترنت، إذا قام باستعراض ذلك وأجرى جميع أعمال التشفير بنفسه. وبعض أنظمة التشغيل يمكنك أن تخبرها على القيام بذلك. وكما تعلمون، فإن لينكس على سبيل المثال،

واحد من بين منتجات شركة ديبيان يأتي الآن مزودًا بشيء يمكنك من خلاله تشغيل مقبض وسوف تقوم بعملية التوثيق بنفسها.

ويوفر بعض الأشخاص برامج يمكنك الالتزام بها في جهازك فقط. وهناك برنامج ما يطلق عليه Stubby ويمكنه القيام بأعمال التوثيق على جهاز الكمبيوتر. ولكن بشكل عام، فإنك تثق بشكل كبير في مزود خدمة الإنترنت الخاص بك أو وحدة الحل في القيام بالشيء الصواب لصالح وعدم الكذب، وأن لا يكون موفر خدمة الإنترنت يعبث بشيء ما في البيانات في طريق عودتها.

متحدث لم يذكر اسمه: نعم، لقد كنت -- حسنًا، نعم، إذا كان بإمكاني أن أضيف لسؤالي. لقد كنت أفكر أكثر، تلتقون بشخص على الشبكة المحلية وربما قام بتسميم والعبث بكل شيء، وربما يقوم بعمل فلترة، ويقوم فقط بالإجابة عن استعلامات نظام أسماء النطاقات أسرع منك.

دان يورك: حسنًا، وهذا هو بالضبط وسيلة الهجوم الذي يمكن أن يحدث، وهذا هو السبب في أنك ترى الكثير من العمل يحدث حول خصوصية نظام أسماء النطاقات، حول بروتوكول نظام اسم النطاق على أمن طبقة النقل، وDNS عبر https، وأيضًا DOH، وكل هذه الأشياء، للنظر في كيفية القيام بذلك تقوم بتشفير الاتصال من جهازك المحلي، كما تعلمون، إلى مُحلل المتكرر الخاص بك حتى تتمكن من الحصول على اتصال آمن هناك، بحيث لا يمكن أن يكون لديك هذا الشخص على شبكتك المحلية الذي يرسل حزمًا. وهذا عنصر آخر من هذه الطبقات، الدفاع في العمق، وطبقات حماية DNS.

وارن كوماري: نعم، أريد المتابعة بشيء ما في ذلك، هناك هجومان مختلفان. يوجد شخص ما على شبكتك، يقوم بأعمال التسميم ثم يعطيك إجابات خاطئة حتى يتمكن من إجبارك على الذهاب إلى المكان الخطأ. ولكن هناك شيء مخيف بنفس القدر من شخص ما على الشبكة ألا وهو مجرد مشاهدة الحزم الخاصة بك، وكما تعلم، لا يساعد الأمر حقًا إذا ذهبت إلى https://alcoholicsanonymous.org، كما تعلمون، وأن كل المحتوى مشفر.

إذا كان بإمكان الناس أن يروا أنك بحثت عن الاسم alcoholics anonymous.org، أو، كما تعلمون، gayrights.org أو منظمة هيومن رايتس ووتش، فإن حقيقة أنك تقوم بحل أسماء معينة، أو حقيقة عدم تشفيرها هي بنفس مستوى ضرر قدرة الأشخاص على رؤية المحتوى الذي تبحث عنه.

دان يورك: روس.

روس موندي: وهذا النوع من الأشياء، الذي كان يصفه وارن، وأحيانًا ما يطلق عليه "هجوم المقاهي"، حيث تدخل إلى المقهى المحلي المفضل لديك، وقد يكون اتصال واي فاي في المقهى مشفرًا، ولكن هذا -- يمكن الوصول إليه مجانًا وأي شخص في هذا المقهى يمكن أن ينضم إلى شبكة واي فاي هذه، ويمكنهم، في الواقع، عمل نسخ أو تقديم إجابات خادعة لاستفسارات نظام أسماء النطاقات الخاصة بك.

إذا كنت كذلك، إذا كانت لديك وسيلة للحماية بداية من جهازك إلى المكان الذي تثق أن المعلومات ستكون دقيقة فيه، فإنك ستكون أقل عرضة للهجوم. وأنا أعلم حقيقة أن هذا أمر ممكن وأن هناك برامج متاحة للتنزيل على الإنترنت تتيح لك القيام بذلك.

دان يورك: ولكي أكون واضحًا، مرة أخرى، ولكي أكون واضحًا أيضًا أكثر من اللازم، فإن DNSSEC تتعلق بضمان حصولك على الإجابات الصحيحة. الأمر بشكل بحث يخص النزاهة والتكامل. ما كنا نتحدث عنه هنا هو طبقات إضافية من تحسينات الخصوصية وسنتحدث عن بعض منها يوم الأربعاء، في جلستنا في الساعة 1:30. سيكون هناك بعض، هناك شيء حول بعض هذه العناصر التي تشكل جزءًا من ذلك. هل اتفقنا جميعًا؟ هل لديك المزيد،؟

متحدث لم يذكر اسمه: نعم، بالفعل، أنا على ما يرام. شكراً جزيلاً لك.

دان يورك: حسنًا، شكرًا. كاثي تقول لي أننا حصلنا على تعليق من شخص عن بعد.

كاثي سكنيت: هذا السؤال من كوزي. هل يمكنك شرح الصفقة التي تمت بين Firefox وCloudflare حول وحدة تحليل DNSSEC، لقد سمعت بذلك من عرض تقديمي سابق.

دان يورك: حسنًا، DoH. لست متأكدًا من ما نحن عليه - إلى أي مدى نريد الوصول إلى هنا؟

ويس هارداكر: لذلك يمكنني تلخيصها من وجهة نظر محايدة.

دان يورك: تفضل، لخصها من وجهة نظر محايدة.

وارن كوماري: أوه، هذا يعني ضمنًا أنني لست كذلك.

ويس هارداكر: المشكلة هي أنني كنت من أعطى الإجابة في المحادثة السابقة، وأحذركم، صححوا لي عندما أخطئ. ما رأيكم في هذا؟ لذلك، هناك نوعان - اسمح لي بالتراجع والإجابة على السؤال السابق، مرة أخرى، بسرعة، أولاً.

هناك طرق متعددة لحماية المحادثة بينك وبين وحدة الحل. حسنًا، دكتور إيفيل. هناك طرق متعددة لحمايتك وصولاً إلى وحدة الحل، وما زال العالم يعمل على ذلك إلى حد ما. وبعد ذلك، فإن فريق عمل هندسة الإنترنت في غضون أسبوعين سوف تعقد المزيد من المناقشات حول ذلك. يمكنك إجراء DNSSEC على عميلك، ويمكنك استخدام شيء مثل DOH، ويمكنك

استخدام شيء مثل DOT، وهناك عدة طرق نحاول بها معرفة كيفية حماية ذلك، وتعمل جميعها بطرق مختلفة.

بالنسبة لمتصفحات الويب، قررت متصفحات الويب نظرًا لأنها ضليعة بالفعل في برتوكول HTTPS، فهم يفهمون هذا البروتوكول، ويفهمون كيفية استخدامه، كما أنهم يمتلكون مكتبات سريعة حقًا تعرف كيفية استخدامها. لقد قرروا أنهم يريدون حقًا إجراء حل نظام اسم النطاق عبر بروتوكول نقل النص التشعبي الآمن وأنهم متحمسون للقيام بذلك. إنهم ينشرونه بطرق مختلفة.

وهكذا، هذا هما الشيئان اللذين أعرفهما، ولا أعرف عن الخطط الأخرى أي شيء، أي Chrome وFirefox. سأبدأ مع Firefox لأنهم برزوا وأعلنوا عنه أولاً. قررت شركة Firefox أنها سوف تدخل في شراكة مع Cloudflare، وهي عبارة وكيل ويب وشركة لديها - لديهم كل أنواع الميزات، كما أنهم أحد الأشخاص الذين يديرون وحدة تحليل للتوثيق من صحة DNSSEC في جميع أنحاء العالم.

كما أنهم يعقدون شراكة مع شركة Cloudflare من أجل إرسال جميع طلبات نظام أسماء النطاقات عبر الويب الخاصة بك إلى Cloudflare، إذا كنت تستخدم Firefox، وفي الوقت الحالي، إذا كنت تستخدم، إذا كنت في الولايات المتحدة. علمًا بأن خطط النشر المستقبلية الخاصة بهم غير مؤكدة حاليًا، لكنها تراجعت إلى مجرد اختبار في الولايات المتحدة هذا الشهر، وفقط مع Cloudflare في الوقت الحالي، ولكن سيكون لديهم مربع قائمة منسدلة سيسمح لك باختيار مزودين آخرين.

أما Google، من ناحية أخرى، وهذا هو المكان الذي يصححه وارن عندما أخطأ، فإن Google، من ناحية أخرى، ستختبر بالفعل موفر خدمة الإنترنت الخاص بك، وتنظر هل يوفر موفر خدمة الإنترنت خدمة HTTP أو HTTPS لنظام DNS. وإذا فعلوا ذلك، وإذا كانوا مدرجين في قائمة موثوق بها، فسيستخدمون DOH للتحدث إلى مزود خدمة الإنترنت. إذا تبين أن هذان الأمران، كما تعلمون، غير صحيحين، فسوف يعودون إلى نظام أسماء النطاقات العادي. ولن يقوموا بإرسال مرور بياناتك إلى جهة خارجية أخرى، ما لم يتغير هذا مؤخرًا.

وارن كوماري: بقدر ما يؤلمني أن أقول ذلك، فإن هذا صحيح بشكل أساسي. أعني أن هناك شيء واحد أود إضافته، هو نهج Chrome. تعتقد شركة Google أنه، كما تعلمون، يجب عليك المتابعة حاليًا أو يجب أن تستمر في التحدث إلى وحدة التحليل الحالية التي تتبعها، لأنه يحتمل أن تفعل أشياء لك مثل الحماية من البرامج الضارة. من خلال التحدث إلى مجموعتك الحالية من وحدات الحل، فإنها لا تغير وحدة الحل الخاصة بك، بل تسمح لك بالحصول على جميع أشكال الحماية الحالية، وتتيح لك إمكانية البحث عن أسماء النطاقات الداخلية، وأشياء من هذا القبيل. وهكذا، هذا هو النهج الذي تتبعه Google بشكل ما.

دان يورك: أعتقد أنه بالنسبة للمستمع عن بعد، أي الذي طرح هذا السؤال، أعتقد أنه من المهم أن نفهم أيضًا وجود بروتوكول، وDOH، وحل نظام اسم النطاق عبر بروتوكول نقل النص التشعبي الآمن، والتي تم تعريفها بواسطة ITF، المعيار RFC 8484. إنه بروتوكول يقوم أساسًا حول كيفية إجراء DNS عبر اتصال HTTPS. يوجد بروتوكول يسمى DOH، ويمكن لعميل DOH -الذي يمكن أن يكون مستعرض ويب، وهذا هو الجمهور الأساسي الآن- التحدث إلى أي خادم DOH. إنها طريقة للحصول على اتصال مشفر وآمن وخاص بين التطبيق ووحدة تحليل DNS. لذلك، يقوم بتشفير ذلك الاتصال. لذلك، فإن DOH باعتباره بروتوكولاً هو ذلك.

والآن فإن DOH، بما أنه يتم نشره في البداية في هذه المراحل المبكرة، فإن هذا هو المكان الذي جاء فيه بعض من هذا الخلاف بسبب هذه الآليات المختلفة والطرق المختلفة التي طلبها الناس. لذلك، أعتقد أنه من المهم أن نفهم أن هناك بروتوكولاً يعمل في طبقة الخصوصية هذه لضمان عدم تمكن أي شخص في المقهى من التقاط جميع بيانات التعريف الخاصة بك حول جميع الأماكن التي تريد الذهاب إليها.

وهذا ما يفعله بروتوكول DOH، وبعد ذلك هناك بروتوكول آخر يسمى بروتوكول نظام اسم النطاق على أمن طبقة النقل، وهو DOT، تم تصميم هذين البروتوكولين للمساعدة في حماية الخصوصية. لذا، فهم موجودان، ويزيدان من مستوى الخصوصية التي لدينا في ذلك. وبعض الأماكن التي يدور فيها الخلاف هو كيف يتم نشرها بالفعل بطرق مختلفة في هذه الأيام المبكرة. روس، أردت أن تقول شيئا، أو - انتظر. وارن؟

وارن كوماري: أشار ويس إلى أنني قد نسيت. إفصاح كامل، أنا أعمل لدى Google، كما تعلمون، وهي الشركة التي تقدم Chrome. لقد قصدت الكشف عن ذلك ولكن نسيت.

روس موندي: لذلك بالنسبة للأشخاص الذين يرغبون في رؤية المزيد، استمعوا إلى المزيد حول هذه المناقشة، في اجتماع ICANN64، أعتقد أنها كانت كذلك، وكانت هناك جلسة موضوعات ذات أهمية عالية لمدة ساعة ونصف، وساعتين تقريبًا، وقد تمت الإشارة إلى بعض من موضوع DOH وDOT، لكنها كانت جلسة طويلة إلى حد ما، وتم تسجيلها، وأنا متأكد تمامًا من أنها متاحة على موقع أرشيف اجتماع ICANN64، بحيث يمكنك مشاهدة بضع ساعات من مناقشة ICANN ذات الصلة هناك.

دان يورك: تعليقات أو أسئلة أخرى؟ أندرو.

أندرو ماكوناتشي: أعتقد أن هذا كان بالفعل في اجتماع ICANN65. ألم يكن هو الأخير، حيث كانت جلسة DOH؟

ويس هارداكر: في مراكش، نعم.

أندرو ماكوناتشي: أجل. أجل. حسنًا.

دان يورك: حسنًا، أي ملاحظة أخرى؟

ويس هارداكر: أود أن أذكر على الأقل، أنني أعمل بالفعل في جامعة جنوب كاليفورنيا، فقط للكشف عن المكان الذي أتبعه.

وارن كوماري: وأعتقد أن من المحتمل أن تكون أشياء أكثر من ذلك، على الرغم من أنني لم أتحقق من الأمر حول DOH، وDOT، وما شابه ذلك في ورشة عمل DNSSEC.

ويس هارداكر: نعم، لدينا جلسة بالفعل يوم الأربعاء حول DoH.

دان يورك: تعليقات أو أسئلة أخرى؟ نعم، هنا في المقدمة، رجل هناك يريد التعليق. ثم رأيتك، تعال إلى هنا أيضًا.

متحدث لم يذكر اسمه: أنا غاي، من الولايات المتحدة. إذن، هل هناك طريقة للقيام باستعلامات DNS الخاصة التي لا يمكن تسوقها من القهوة، بحيث لا يتم السماح بالتطفل، لأن استعلام DNS نفسه مشفر بطريقة أو بأخرى؟

دان يورك: أجل. وهنا بالنسبة لكليهما، مرة أخرى، أي DOH أو DOT، تلك هي التقنيات التي تسمح لك بالانطلاق والقيام بذلك، ويمكنك الاتصال من خلال، أيضًا إذا كنت ترغب في استخدام تلك الأشياء مباشرة، فيمكنك القيام بها من متصفح الويب الخاص بك. إذا قمت بإعداد Chrome أو Firefox من أجل الاستخدام، فيمكنك إعدادهما الآن لاستخدام DOH ويمكنك إخبارهما عن الخادم الذي سيتم الاتصال به. إذن، ويمكنكم الانطلاق والقيام بذلك الآن.

ويمكنك أيضًا الانتقال إلى DNSprivacy.org، اتفقنا؟ موقع DNS-privacy.org، حيث توجد سلسلة كاملة من البرامج المختلفة الأخرى التي يمكنك تثبيتها. ويمكنك تثبيت شيء يسمى

Stubby على نظامك المحلي، والذي سينطلق ويشفّر كل استفساراتك إلى خوادم DOT المعينة الموجودة. إذن، يمكنكم الانطلاق والقيام بذلك الآن. يمكنك أيضًا تشغيل خادم DOH أو DOT الخاص بك إذا كنت ترغب في ذلك. ويمكنك تشغيل ذلك بنفسك، في مكانك وإعداد ذلك بهذه الطريقة. فمن الممكن القيام بذلك.

وارن كوماري: ويمكنك أيضًا تشغيل VPN، كما تعلمون، إذا أردت حلاً سهلًا وسريعًا الآن لكل شيء.

دان يورك: نعم. نعم، أنت. تعليقات أو أسئلة أخرى؟ نعم، هناك في الخلف.

روكيو دي لا فوينتي: سؤالي يتعلق بمسألة محو الأمية الرقمية. عندما نتحدث عن تثقيف وتعليم المستخدمين أو المسجلين، هل يجب أن نوضح لهم أهمية DNSSEC لنطاقاتهم عند التسجيل؟ لأنه عندما نتحدث عن مزودي خدمة الإنترنت، أو السجل أو أمناء السجلات -- ليس أمين السجل، بل السجلات، أليس كذلك؟ لكن عندما نتحدث عن ذلك، فهل سيساعد ذلك على نشر DNSSEC؟ ما رأيكم في ذلك؟

دان يورك: حسنًا، أعتقد أن كل واحد منا هنا وآخرون هنا سيقولون، "بالتأكيد". من المؤكد أننا نشجع الناس على تضمين ذلك كجزء من ذلك العمل، كما تعلمون، ونقول فقط إنه بينما تقوم بالترويج لنطاقك هناك وأنت تقوم بنشره وتعميمه، فيجب التوقيع عليه.

ومرة أخرى، فإن بعض أمناء السجلات، وأنا لا أعرفهم في الأرجنتين، لكن بعض أمناء السجلات الموجودين وصلوا إلى هذه النقطة، كما أن أمناء السجلات ومقدمو خدمات استضافة DNS وصلوا إلى النقطة التي جعلوا فيها DNSSEC أمرًا سهلاً كما تعلمون، باختيار مربع اختيار، أو تحريك مفتاح، أو القيام بشيء ما آخر.

وهذا حقًا في العالم المثالي، حيث نريد أن ننطلق جميعًا، في جانب التوقيع، حيث أصبح مجرد شيء بسيط وسهل للغاية حتى أنه لا يتعين على المستخدم النهائي المشاركة بالفعل بطريقة ما في هذا الأمر. لكننا نشجع الناس على الخروج إلى هناك وتوقيعهم لأنه يضمن من منظور العلامة التجارية، من وجهة نظر السمعة، أنه يضمن وصول الناس إلى المواقع التي تقوم بوضعها في DNS.

وارن كوماري: إذن، هل يمكنني أن أختلف قليلاً؟

دان يورك: وارن يمكن أن يختلف، بالطبع.

وارن كوماري: يمكن لوارن أن يختلف مع أي شيء لأنه يحب الجدال. لذا، فهذا يعتمد على عوامل، مثل عند أي النقطة في دورة محو الأمية الرقمية يكون ذلك. أعتقد أننا جميعًا نقول بأن DNSSEC شيء جيد، لكن هل هو أهم شيء بالنسبة لمستخدم جديد على الإنترنت؟ ربما لا. هل هو الشيء الأكثر أهمية عندما يسجل شخص ما نطاق ما؟ قد يكون الأمر كذلك، لكنني أعني أن هناك الكثير من الأمور الأمنية الأخرى التي تعتبر ذات أهمية حقًا والتي تحتاج إلى تصحيح. وهذا يتناسب مع جانب محدد.

دان يورك: حسنًا، وارين. كان ذلك جانب خلاف جيد. تفضل.

روكيو دي لا فوينتي: لهذا السبب، كنت أفكر في ذلك أيضًا. لأنه عندما تفكر في ما يتعلق بالمحفزات، وكما هو الحال بالنسبة لنا، فإننا نشارك نوعًا ما في ICANN وحوكمة الإنترنت. وإذا لم تكن لديك خلفية تقنية، فيجب عليك قضاء بعض الوقت والجهد في فهم مدى أهمية DNSSEC. لذلك، فإن

المسجل أو المستخدم، يفكر في شركته أو أيًا كان. مثل، كيف لنا أن نقول مثلاً، "حسنًا، هذا مهم. ربما سيكون نطاقك أغلى ثمناً قليلاً، لكن لديه الإنترنت أو الأمان"، أليس كذلك؟

دان يورك: أجل. هذا جزء من التحدي وبصراحة تامة هذا هو السبب في أننا نعمل في أماكن كثيرة مع مزودي نظام أسماء النطاقات أو مزودي استضافة نظام أسماء النطاقات أو أمناء السجلات الذين قد يكونوا في كثير من الأحيان هم نفس الموفرين ويشجعونهم على جعل هذا الأمر يحدث، فقط من خلال التوقيع على كل شيء، كما يفعل بعض مزودي خدمة استضافة نظام أسماء النطاقات، حيث يقومون فقط بالتوقيع عليه بشكل افتراضي. أو للتسهيل على الناس فهم ذلك والقيام بذلك. ومن الناحية المثالية، جعل هذا الأمر بدون تكلفة، رغم أن نماذج الأعمال تختلف في أماكن مختلفة، كما تعلمون.

لأن هذه وجهة نظرك، وارين، وأنا أتفق مع وارين، أنه في المخطط الكبير للأشياء التي يحصل عليها شخص ما على الإنترنت في مكان جديد، وهذا أحد تلك الأشياء الأخرى التي لديهم على قائمتهم. لكنها قد لا تنشأ، اعتمادًا على مستوى قدرتها على التحلي بالقدرة على الفهم وقدرتهم على التعامل معها، فقد لا ترتفع إلى القمة.

لكن لهذا السبب، ومن الناحية المثالية، فهي مجرد شيء موجود في البنية التحتية. وكما تعلمون، فإنه يجري التعامل معها وفق تلك المستويات. هل ستختلف معي بعد الآن، وارين؟ لا؟ حسنًا، جيد. فسوف يوضح لكم. تعليقات أو أسئلة أخرى؟ لدينا وقت لنحو سؤال واحد أو اثنين آخرين. لا؟ آه، حسنًا، السيد ليفين هنا. أنا أقول ذلك لأني أعرف جون جيدًا.

جون ليفين: لا، هذا في الواقع مجرد إعلان تجاري.

دان يورك: إعلان تجاري؟

جون ليفين: أجل. قبل قليل، ذكر عدد قليل منكم ما قد يكون تشفير الكم -- ما قد يكون له من تأثير على DNSSEC، ومن قبيل الصدفة المدهشة، هناك حديث عن هذا الموضوع بالضبط، وهو الحديث الأخير في يوم التكنولوجيا غدًا.

دان يورك: ممتاز.

جون ليفين: نعم. الخبر السيء هي أن الشخص الذي يبلغنا به مغرور وثرثار، لكن ليس هناك ما يمكنك فعله حيال ذلك.

دان يورك: حسنًا، شكرًا لك، جون.

ويس هارداكر: نحن نفترض أنك أنت، جون وأنك على ما يرام.

دان يورك: حسنًا، صحيح. حسنًا. إذن، سيقوم جون بالحديث غدًا في نهاية يوم التكنولوجيا، وبالمناسبة، إذا كنت جديدًا، وأرى عددًا من الزملاء الذين قالوا إنهم زملاء جدد، فسيكون غدًا يوم التكنولوجيا، حيث يوجد عدد من الجلسات المختلفة التي تجري في إحدى هذه القاعات.

لست متأكدًا من أي منها، ولكن إذا نظرت في الجدول الزمني ليوم التكنولوجيا، وهناك الكثير من الموضوعات المختلفة التي تتراوح -على ما أظن- ما بين تشفير الكم، حول هذا الموضوع، إلى هجمات DDoS أو هجوم حجب الخدمة الموزعة، إلى أنواع أخرى مختلفة من الأشياء، أو مواضيع متنوعة ومختلفة. أنا لم أطلع على الجدول الزمني لهذا الاجتماع لهذا الأسبوع، لذلك فأنا لا أعرف حتى. لكن على أية حال، هناك الكثير من الجلسات الجيدة الموجودة هناك أيضًا.

وارن كوماري: سيكون ذلك في القاعة 516C.

دان يورك: أوه ، استمعوا لذلك. ممتاز. لم نجد ذلك، وهو الساعة 10:30 موعد البدء غدًا. هل هناك شيء آخر؟ حسنًا. إذن، إذا لم يكن الأمر كذلك، أود أن أشكركم على اهتمامكم وأيضًا، إذا كنتم مهتمين بالمزيد، فحضوركم محل ترحاب والتحدث إلى أي منا، فسنكون موجودون لبضع دقائق أخرى.

وأكرر مرة أخرى، يوم الأربعاء في الساعة 1:30 في القاعة 517C، وهي القاعة المجاورة، حيث سيكون لدينا ورشة عمل DNSSEC، والتي سوف تغطي مجموعة من الموضوعات. ويمكنكم رؤية جدول الأعمال إذا انتقلتم وألقيتم نظرة على الموقع على برنامج تحديد الجدول وكل تلك الأشياء. إذن، شكرًا جزيلاً لكم وأتمنى أن تستمتعوا بأسبوعكم هنا في ICANN.

[نهاية التدوين النصي]