مراكش - DNSSEC للجميع: دليل للمبتدئين
الأحد، 06 مارس، 2016 – من الساعة 04:45 م إلى الساعة 06:15 م بتوقيت غرب أوروبا
ICANN55 | مراكش، المغرب

جولي هيدلوند: أهلاً بكم جميعًا. أنا جولي هيدلاند من طاقم ICANN. سنبدأ جلسة DNSSEC للجميع خلال بضعة دقائق، لذا أشجعكم رجاء للدخول هنا في القاعة وأخذ مقاعدكم. اجلسوا في الأمام بشكل جيد وأغلقوا الغرفة حتى تتمكنوا من الاستمتاع بالمسرحية الهزلية الرائعة ورؤيتها بشكل أفضل.

ثم سيكون لدينا الكثير من الوقت للأسئلة. ستكون لدينا بعض مكبرات الصوت هنا حتى نتمكن من تلقي أسئلتكم كذلك. لكن رجاء، تعالوا، اقتربوا، سنبدأ في غضون لحظات. أهلاً بكم مجدداً في جلسة DNSSEC للجميع: دليل للمبتدئين.

مرحبًا بكم جميعًا. برجاء الاستمرار في المجيء للقاعة وإيجاد مقاعدكم. نحن فقط نتأكد من أن الجميع يرجع هنا، ثم سنبدأ حينها. هذا DNSSEC للجميع: جلسة دليل للمبتدئين، وهو ما ترونه هناك في الأعلى أمامكم على الشاشة. شكرًا.

دان يورك: حسنًا. طاب مساءكم. كيف حالكم جميعاً؟ كم منكم كان في هذه القاعة طوال اليوم؟ أجل. حسنًا. حسنًا. حسناً، اسمي دان يورك، وسنتحدث هنا عن DNSSEC للجميع. أعتذر عن التأخير. ظننا أن لدينا فيديو في هذه القاعة. سنقوم بمسرحية هزلية، لذا قلنا للأشخاص عن بعد بأنه يمكنهم مشاهدة الفيديو، لكنه تبين أنه ليس لدينا فيديو. لقد كنا نحاول رؤية إذا كان يمكننا فعل شيء آخر - استخدام جهاز iPhone، أو القيام بنوع من الفيديو أو شيء - لكن ذلك لم ينجح. لذلك فإننا فقط سنقوم بالمتابعة والمضي قدماً. جميعكم الذين هنا في القاعة يجب أن تكون لديكم تلك الخبرة.

أوه، تم تذكيري - لدينا الترجمة، لذا سيتوجب علينا الحديث بشكل أبطأ. أنا أسوأ ضحية لذلك. لا تريدون مني الحديث بالفرنسية. بمجرد ما أتجاوز قولي بالفرنسية "اسمي دان، وأنا أمريكي،" فأنا نوعاً ما أنتهي هنا. "ليمون هندي." أعرف تلك الكلمة بالفرنسية. أنا أحاول.

على أي، كم منكم قد سمع أي شيء حول أمن DNS أو حول DNSSEC؟ القليل من الأشخاص المتناثرين هنا. حسنًا. كم منكم سجل نطاقاً مع DNSSEC؟ حسنًا. كم منكم يسير محللي التحقق خاصته؟ كم منكم ليست لديه أية فكرة حول من هم محللو التحقق؟ جيد. حسنًا. أنتم الأشخاص المناسبون حقاً لهذا.

إذا ما نظرتم إلى جدول الأعمال - ومن المفترض أنكم استلمتم نشرة صغيرة، نسخة مطبوعة، هنا في الأسفل. إذا لم تكونوا قد استلمتم، فلا تزال لدينا البعض منها. في هذه الجلسة، سأتحدث قليلاً عن نظرة حول ماذا كان يمكن أن يكون تاريخ DNSSEC والقيام بقليل من التوضيح حول ما يجعله مميزاً، وما المهم بشأنه.

ثم سنتحدث عن بعض مبادئه وسنعطي بعض أمثلة الحالة، وأمور مثل ذلك. خلال السير قدماً، ترون بالفعل الأشخاص يلبسون بعض القمصان قصيرة الأكمام. سنقول قصة قصيرة وسنستمتع قليلاً بهذا مع مضينا قدماً.

سأبدأ، أقول - أوه، أنا أدفع في الاتجاه الخاطئ. ها نحن ذا. أنا مرتبك. سنقوم برحلة صغيرة إلى الماضي، ونذهب إلى أصول DNSSEC في سنة 5000 قبل الميلاد. حسنًا؟ هل أنتم مستعدون؟

هذه أوغوينا. حسنًا؟ تعيش في كهف في أحد جوانب جراند كانيون. وهذا أوغ. يعيش في كهف في الجانب الآخر من جراند كانيون. هناك طريق طويلة أمامهم إذا أرادوا الذهاب والحديث مع بعضهم البعض. عليهم عبور كل الطريق نحو الأسفل وكل الطريق نحو الأعلى. لم يكونوا يتحدثون كثيراً عن ذلك.

وفي أحد الزيارات، لاحظا أن الدخان يتصاعد من النار نحو الأعلى. وفكرا في هذه الفكرة. قالا، "أوه، مهلاً. انتظر. يمكننا بدء استخدام إشارات الدخان والمحادثة من جانب إلى آخر."

لن بعد ذلك، في أحد الأيام، انتقل رجل الكهوف المزعج كامينسكي إلى جوار أوغ، وبدأ في إرسال إشارات الدخان، أيضاً. الآن أوغوينا المسكينة على الجانب الآخر جد محتارة. فهي لا تدري ما هي الإشارات التي يجب عليها النظر إليها. ما هي الإشارات التي تتضمن المعلومات الصحيحة؟ إنها لا تعلم. إنها جد محتارة.

لذا انطلقت للذهاب والصعود ومحاولة تصور ما الجواب الممكن لهذا. قام أوغوينا وأوغ بالتشاور مع شيوخ القرية، وكان أحدهم هو رجل الكهوف ديفي، والذي كانت لديه فكرة صغيرة حول ما يجب القيام به.

جرى وذهب إلى خلف كهف أوغ. خلف ذلك الكهف، وجد هذا الرمل الأزرق الغريب الذي تم إيجاده فقط في كهف أوغ.

الآن جرى خارجاً، ورمي بعض هذا الرمل في النار. وتحول الدخان بشكل مذهل إلى اللون الأزرق. فجأة، الآن قام أوغوينا وأوغ بتجاوز الأمر بسعادة عبر إشارات الدخان لأنها تعرف أن الدخان الأزرق هو الذي تريد التركيز عليه، ويمكنها إهمال كل المحاولات الأخرى التي تحصل.

باختصار شديد، هذا ما نقوم به من خلال DNSSEC. نحن نوفر نوعاً من الدخان الأزرق، شيئاً فريداً يمكنكم تقديمه يقول، "هذه هي المعلومات التي أضعها هناك." لا أحد آخر لديه ذلك النوع الخاص من لون الدخان. لا أحد آخر لديه ذلك. لون مارك قد يكون أحمر ولونك قد يكون أخضر ولونك قد يكون برتقالياً أو ما شابه. لدى كل شخص لونه الخاص. لدى كل واحد منكم طريقة فريدة للقيام بذلك. وتوفر DNSSEC طريقة للتفريق بين المعلومات وضمان أنكم تحصلون على المعلومات الدقيقة هناك.

للنظر في هذا بتفصيل أكثر قليلاً، على مستوى عال جداً، إذا رأيتم هذه الأنواع من صور DNS، والتي هي DNS نفسه، فلدينا جذر ذلك. لدينا عدة TLDs (نطاقات المستوى الأعلى) مختلفة حاصلة هنا، ثم لدينا عدة نطاقات المستوى الثاني مختلفة هنا. هذا هو هيكل يصف الأمر.

كل منا، سواء ذهبنا إلى موقع، أو حينما نذهب لإرسال بريد، أو حينما نقوم بأي شيء مثل هذا، فإننا نستخدم محللاً. هناك محلل، أو محلل DNS، على هاتفنا الذكي، وعلى حاسبنا المحمول، وعلى أي شيء آخر. هناك محلل يأخذ اسم النطاق، سواء كان ذلك النطاق google.com أو nic.ma أو bank.com أو أي شيء. إنه يأخذ اسم النطاق، ويحوله إلى عنوان IP، ويستخدم ذلك العنوان IP من أجل التواصل. ذلك ما يقوم به DNS: فقط تلك الأنواع اللامتناهية من عمليات البحث.

كل جهاز لديه محلل. يحصل المحلل على تلك المعلومات مجدداً ثم يحتفظ بها لفترة من الزمن. لديه تخزين مؤقت، كما يسمى محلياً. ويقوم بتخزينه لفترة من الزمن. قد تكون ساعة. وقد تكون يوماً. وقد تكون أسبوعاً. إنه يعلم أن عنوان IP لمؤسسة ICANN، من أجل www.ICANN.org، هو أي شيء. إنه يعلم ذلك. ويخزن ذلك. ويحتفظ بذلك.

السؤال الذي تصل إليه، أو التحدي، هو أن DNS ليس لديه أمن في شكله الأصلي. مارك هناك، يجلس هناك، قد يأتي ويمكنه أن يحاول الدخول وأن يقول لأحد آخر ما هو عنوان IP لموقع www.ICANN.org. هذا السيد الجالس خلف هنا مباشرة سيثق فيه لأن مارك أقرب قليلاً، لذا يمكنه أن يخبر ذلك السيد قبل أن أستطيع ذلك. هناك انتظار هنا.

هذا جزء مما هو DNS. هذا الشيء يسمى التسميم هنا؟ نحن لا نستخدم السم في الواقع. سوف يكون ذلك سيئاً. ما نقوم به حقاً هو عبر التسميم - ما يعنيه ذلك هو، إذا كان محلل ذلك السيد سيحصل على المعلومات من مارك قبل معلوماتي، فسيستخدم تلك المعلومات إلى حين انتهائها. لديه وقت ليعيش على ذلك؛ إلى غاية انتهائه. سنرى هذا بعد قليل حين نقوم بمسرحيتنا الهزلية الصغيرة.

سأقوم بجلب ممثلي DNSSEC هنا. لدينا فريق. أجل. أوه. إذن لدينا فريق صغير هنا يلبسون قمصانهم قصيرة الأكمام. أوه، ولدينا ميكروفون ثان، صحيح؟

شخص غير محدد: أجل.

شخص غير محدد: [غير مسموع] ميكروفون ثان؟ ها نحن ذا.

دان يورك: لنتحقق من هذا. نعم. حسنًا. انتظار. نعم، حسنًا. أنا لست الراوي عادة. حسنًا. أنت ISP. يجب على تقديم - حسناً. سنقوم بتنظيم هذا. ما سنقوم به هو أننا سنقوم بمسرحية هزلية صغيرة - هل ستأتون يا رفاق؟ حسنًا. ماذا سنفعل؟ حسنًا. هل كل شيء على ما يرام؟ حسنًا.

شخص غير محدد: تنظيم ذاتي.

دان يورك: تنظيم ذاتي. [غير مسموع]. يجب علي أن أقدم. هذا ويس هارداكر، يلعب دور المستخدم جو، والذي هو أي أحد منا يتصفح على الإنترنت، ويقوم بشيء مثل هذا. لدينا دور مقدم خدمة الإنترنت له يمثله جاك لاتور هناك. لدينا أندرو يلعب دور خادم الجذر في مركز كل DNS. وارين في دور خادم كوم، وروس في دور خادم البنك، ويبدو أننا نحصل على إكسسواراتنا. هل جمعنا إكسسواراتنا؟

شخص غير محدد: نعم.

دان يورك: حسنًا. حسنًا. DNS في قاعدة البيانات الضخمة الموزعة هذه في الأنظمة هنا. لذا سنقوم بهذه المسرحية الهزلية الصغيرة. الآن، أولئك منكم الذين يعرفون الكثير عن DNS قد يعلمون أننا نأخذ بعض الحريات بخصوص كيف يعمل بالضبط. حسناً؟ هذا لإعطاء فكرة عامة عما يحصل هنا.

سنمر عبر مجموعة من القطع المختلفة، والجزء الأول هو أننا سنقوم فقط ببعض الخدمات المصرفية عبر الإنترنت. المستخدم جو هنا يريد الذهاب إلى بنكه. يريد الذهاب إلى www.bigbank.com. هذا ما سيحدث في فضاء DNS.

ويس هيرداكر: حسناً، أحتاج أن أذهب لأدفع فاتورة الكهرباء خاصتي لأن الأجل اقترب من الانتهاء ويجب على أن أدفع ثمنها، لذا سأكتب اسم بنكي على متفح الإنترنت خاصتي والذهاب إلى www.bigbank.com لأنني أريد دفع فاتورة الكهرباء خاصتي. لكنني لا أعرف حقاً أين يوجد ذلك على الإنترنت، لذا يجب على أن أسأل ISP خاصتي، أي مزود خدمة الإنترنت خاصتي. أين يوجد ذلك، رجاءً؟

جاك لاتور: شكرًا لك، المستخدم جو. أنا خادم اسم تكراري. لقد استيقظت للتو. ولا أعرف أي شيء، لذا من الواضح أنه علي الذهاب والبحث عمل هو bigbank.com. سأرد عليك بجواب.

الشيء الوحيد الذي أعرفه هو أين يوجد الجذر على الإنترنت، لذا سأذهب إلى الجذر. مرحباً أيها الجذر. أنا أبحث عن www.bigbank.com. هل تعرف أين يوجد ذلك؟

أندرو: المعذرة. لا أعرف أين يوجد www.bigbank.com. لكنني أعرف أين يوجد com. إنه على 1.1.1.1.

جاك لاتور: ممتاز. لذا سأذهب إلى 1.1.1.1. شكرًا. مرحباً يا com. أنا أبحث عن www.bigbank.com. هل تعرف أين يوجد ذلك؟

وارن كوماري: عذرًا. لا، أنا لا أعرف. لكنني أعلم أين يوجد bigbank.com. إنه على 2.2.2.2. يجب عليك الذهاب وسؤاله.

جاك لاتور: نعم، شكرًا. 2.2.2.2. مرحباً يا BigBank. أنا أبحث عن www.bigbank.com. هل تعرف أين يوجد ذلك؟

روس موندي: حسناً، في الواقع، أنا أعلم أين يوجد www.bigbank.com. إنه على 2.2.2.3.

جاك لاتور: أوه. جواب. شكرًا. مرحبًا جو. عنوان IP هو 2.2.2.3.

ويس هيرداكر: شكرًا جزيلاً. سمكنني الذهاب لإرسال 1000 دولار إلى شركة الكهرباء خاصتي الآن.

دان يورك: حسنًا. فلنمنحهم جولة تصفيقات. الآن، فكروا فيما كان يحصل هنا. هذا التفاعل - المستخدم جو يتكلم مع ISP خاصته إلى المحلل - هذا يحصل ملايين المرات في الثانية مع كل ما نقوم به، في كل مرة نضع صفحة على الويب، وكل مرة بقوم بأي نوع من التفاعل مع أي نوع من التطبيقات. كل شيء يجب أن يكون له عنوان IP يقوم بهذا النوع من الأمور.

الآن، بالطريقة الحقيقية التي يعمل بها هذا، من جانب التخزين المؤقت، سيبدأ ISP في الحصول على الحصول على كل هذه المعلومات، وسيكون ISP قادراً على الرجوع إلى المستخدم جو بسرعة ليقول، "أوه، نعم. أعلم أين يوجد هذا،" لأن المستخدم جو قد ذهب وخزن كل هذه المعلومات بشكل مؤقت.

لكن ذلك لا يساعد قصتنا، لذا فقد أزلنا فقذ هذه الحقيقة اليوم للقيام بهذا.

والآن، هل الجميع مستعدون للعنصر الآخر؟ العنصر الآخر جاهز. حسنًا. الآن سنظهر ما سيحصل هنا مع DNS العادي. إذن DNSSEC لم يدخل إلى هنا أبداً. هذا فقط هو نفس الأمر البسيط القديم الذي يحصل اليوم.

سيقوم جو بالأمر مجدداً، لكن هذه المرة سترون فقط شيئاً آخر يحصل. تفضل، جو.

ويس هيرداكر: يا إلهي. نسيت أن أدفع فاتورة الماء خاصتي. يجب على أن أدفع فاتورة الماء خاصتي، لذا سأرجع إلى www.bigbank.com. لكنني لا أتذكر أين يوجد لأنني لا أحتفظ بأي شيء. هل يمكنك رجاءً، يا ISP، أن تخبرني أين يوجد www.bigbank.com؟

جاك لاتور: نعم، شكرًا. لقد استيقظت للتو هذا الصباح، لذا لا أعلم أي شيء. لكنني أعرف أين يوجد الجذر. مرحباً أيها الجذر. أنا أبحث عن bigbank.com. هل تعرف أين يوجد ذلك؟

أندرو: المعذرة. لا أعرف أين يوجد www.bigbank.com. لكنني أعرف أين يوجد com. إنه على 1.1.1.1.

جاك لاتور: نعم، شكرًا. 1.1.1.1. مرحباً يا com. أنا أبحث عن bigbank.com. هل تعلم أين يوجدون؟

وارن كوماري: انتظر! لقد أخبرتك للتو. لا أعرف أين يوجدون، لكن bigbank.com يوجد هناك: 2.2.2.2.

جاك لاتور: المعذرة. لست ذكياً جداً. سأستمر في طرح الأسئلة. مرحباً يا BigBank. أنا أبحث عن www.bigbank.com. هل تعرف أين يوجد ذلك؟

جاي ديلاي: أوه نعم، أعلم. يمكنك أن تجد www.bigbank.com على 6.6.6.6.

جاك لاتور: أوه، كم ذلك رائع؟ شكرًا جزيلاً لكم. مهلاً، جو. www.bigbank.com هو على المصرفي IP 6.6.6.6.

ويس هيرداكر: أوه، شكراً جزيلاً. يا للهول، فاتورة الماء خاصتي لهذا الشهر باهظة. تقول أنني مدين بمليون فرنك سويسري. لكنني أظن أنني سأدفعها.

دان يورك: حسنًا. فلنمنحهم جولة تصفيقات أخرى هناك. الآن، ستلاحظون أن ما حصل هنا هو أن جاي هناك، والذي يلعب دور الدكتور إفيل، أنجز ما يمكننا تسميته هجوم رجل-في-الوسط. لقد قفز إلى هنا وتفوق على روس في إعطاء الجواب الصحيح. الأمر يتعلق بالسرعة. كان هو الأسرع في الوصول إلى هناك، وقام بذلك بالفعل. كان بوسعنا فعل الأشياء مثلما فعل هجوم الحرمان من الخدمات، حيث نقوم نوعاً ما بدفع روس خارجاً أو ما شابه، لكن نوعاً ما كان جاي أول من وصل هناك وأعطى الجواب.

ذلك هو الهجوم الأساسي الذي نحاول تجنبه من خلال DNSSEC. نحن نحاول منع أي أحد من دفع تلك المعلومات هناك.

لاحظوا أن هذا كله حصل قبل حتى أن يتصل جو بالموقع. لم يتصل ولم يحصل على شواهد TLS. لم يقم بأي شيء مثل ذلك. نحن فقط نحاول إيصال جو إلى الموقع الصحيح. هذا كل ما نحاول القيام به.

حسنًا. إذن الآن – حسناً. لقد بدأوا بالفعل هنا. ها نحن ذا. حسنًا. في حين كنت أتكلم.

لفعل DNSSEC، ولفعل أمن DNS، لدينا جانبان. هناك جانبان لهذا. هناك جانب التوقيع، والذي هو أن الأشخاص الذين يشغلون النطاقات لهذه المعلومات عليهم وضع توقيعات تشفيرية. عليهم توقيع نطاقهم. إنه ينطوي على برمجيات تذهب وتولد هذه التوقيعات، والتي تقول أساساً، "هذه المعلومات صحيحة تماماً."

إذا فكرتم في الأمر مثل زجاجات الدواء التي لديها تلك الرقاقة في الأعلى، ذلك النوع من الرقاقة المقاومة للغش، حيث لا يمكنكم أساساً فتح الزجاجة حتى تمزقوا تلك الرقاقة هناك - يقول أن تلك الحبوب أو أي شيء تمت تعبئتها من طرف المصنع - والذي هو نفس نوع الشيء الذي نفعله بهذه التوقيعات. إننا نقول، "هذه المعلومات هي ما تم وضعه في البداية."

إذن فقد وقعوا أنفسهم، ثم مرروا بعض المعلومات من BigBank إلى TLD، والذي يمررها بدوره إلى الجذر. إنها تنشئ سلسلة ثقة هنا حتى لا يتمكن مهاجم بالضرورة من ادعاء أنه كان هناك توقيع والقيام بذلك.

الآن، ذلك هو الجانب الأول. الجانب الثاني هو أن ISP خاصتنا هنا يجب عليه التحقق من التوقيعات لأنهم إذا وقعوا، فذلك رائع. لكن إذا لم يتحقق، فماذا إذن؟ ليس هناك أي أمن إضافي. سوف يقوم بما نسميه التحقق - أو التحقق DNSSEC. سيتحقق من التوقيعات ويتأكد من أنها صحيحة.

مشهدنا التالي، المشهد 3 - في الواقع، لا. المشهد 3 قمنا هنا بتوقيعنا وتحققنا وكل ذلك. نحن متواجدون جميعًا. الآن سننتقل إلى المشهد 4 ورؤية كيف سيعمل هذا مع DNSSEC القادم.

ويس هيرداكر: حسنًا. اليوم أريد الذهاب وإرسال مكافءة إلى صديقي، دان، والذي يقوم بأداء رائع وأظن أني سأرسل إليه ليرة إيطالية. سأذهب إلى www.bigbank.com وأحاول إرساله له، إلى صديقي، بعض المال. هل يمكنكم مساعدتي؟ وأنا الآن مسجل الدخول مع ISP الذي يحتوي على محلل تحقق.

جاك لاتور: آه، اتخذت قراراً حكيماً هناك. شكرًا. إذن تريد الذهاب إلى bigbank.com؟

ويس هيرداكر: نعم، تفضل.

جاك هيرداكر: شكرًا. حسنًا. لا أعرف أي شيء. لقد استيقظت للتو، لذا سأذهب إلى الجذر مجدداً وسأسأله أين يوجد www.bigbank.com.

أندرو: المعذرة. لا أعرف أين يوجد www.bigbank.com. لكنني أعرف أين يوجد com. إنه هنا على 1.1.1.1. اسمح لي أن أوقع على ذلك. ها نحن ذا.

جاك لاتور: أوه، نجح ذلك. توقيع صحيح. شكرًا. إنه صحيح. سوف أذهب إلى com. مرحباً يا com. أريد أن أذهب إلى www.bigbank.com. هل تعرف أين يوجد ذلك؟

وارن كوماري: أنا أعرف في الواقع أين يوجد bigbank.com. لا أعرف أين يوجد www.bigbank.com. هل تريد أن تعرف أين يوجد bigbank.com؟ يسعدني أن أقول لك. إنه على 2.2.2.2. هذا توقيعي الذي يبين أنه حقيقي.

جاك لاتور: اسمح لي أن أتحقق من ذلك التوقيع. اسمح لي أن أتحقق منك. نعم، نجح ذلك. ممتاز. شكرًا. مهلاً، نحن جيدون. حسنًا. فلننتقل إلى bigbank.com. مرحباً يا bigbank.com. أريد أن أذهب إلى www.bigbank.com.

روس موندي: أعتقد ذلك. نعم. إنه على 6.6.6.6.

جاك لاتور: شكرًا جزيلاً لكم. شكرًا. اسمح لي أن أتحقق من التوقيع. مهلاً! إنه خاطئ! أخرج من هنا! هل يمكنهم تصديق ذلك؟

شخص غير محدد: شكراً لك، السيد ISP. أنا أعرف أين يوجد www.bigbank.com. إنه على 2.2.2.3، وسأوقعه. ها نحن ذا.

جاك لاتور: شكرًا جزيلاً لكم. اسمح لي أن أتحقق من التوقيع. اسمح لي أن أتحقق منك. نعم، إنه ينطبق. شكرًا. كل شيء جيد.

حسناً، المستخدم جو، أنا مطمئن أن عنوان IP للموقع bigbank.com هو 2.2.2.3.

ويس هيرداكر: ممتاز. شكرًا جزيلاً لكم. سمكنني الذهاب لإرسال تلك الليرة إلى صديقي، دان، الآن. شكرًا.

ها هم.

دان يورك: رائع. شكرًا. وكم قيمة الليرة؟ متى يمكنني توقعها؟ شكرًا. فلنقم بجولة تصفيقات.

الآن، السؤال موجه لكم: ما الذي توجب على المستخدم جو القيام به في هذا السيناريو؟ هل كان يتعين عليه القيام بأي شيء؟

سيدة غير معروفة: لا.

دان يورك: لا. لقد عمل فقط له في الخلفية. ISP - ما الذي كان يتوجب على ISP القيام به؟

متحدثون غير معروفون: [غير مسموع]

دان يورك: التحقق. التحقق من التوقيعات. كل الأمور الأخرى حصلت بين خوادم الأسماء التي كانت هناك. حسنًا؟ هذا على مستوى بسيط، ما حصل في DNSSEC. حسناً؟ هذا ما نحاول القيام به: منع الدكتور إفيل من القفز هناك وتوفير ذلك العنوان IP.

الآن، إن الأمر أكثر تعقيداً قليلاً من هذا. حسناً؟ سوف نتحدث قليلاً عما يتعلق بذلك. لكن هذه هي العملية الرئيسية. ما رأيكم؟ هل يبدو ذلك جيداً لحد الآن؟ حسنًا؟

لنراجع فقط مجموعة من الأمور هنا. نعم، لقد قاموا بهذا. قاموا بهذا. لقد قمنا بذلك. قمنا بالشيء الأزرق. قمنا بهذا، ونحن هنا. حسنًا.

فقط بضعة كلمات تحدثنا عنها. نتحدث عن التوقيعات الرقمية، ونتحدث عن المفاتيح، والحصول على المفاتيح التي تذهب مع معلوماتك. حين تنشر معلوماتك في DNS، تماماً كما فعلت دائماً، فإنك أيضاً تنشر توقيعاً. تولد هذا. البرمجية هناك التي فعلت هذا. أنت تولد هذا وتنشر ذلك. كل تلك المعلومات يتم تخزينها في DNS.

هناك جزء إضافي لم نتحدث عنه حقاً. عندما يذهب المحلل إلى الجذر ويطلب تلك المعلومات ويرجع توقيعاً، فإن المحلل قد علم أيضاً بشأن مفتاح الجذر. يعلمون المفتاح الذي سيكون وراء كل ذلك.

أحد الأمور التي ستسمعها يتم الحديث عنها في عالم DNSSEC هي مناقشة مستمرة حول انتقال مفتاح الجذر، والذي يذهب إلى تغيير ذلك المفتاح، شيء سنتحدث عنه أكثر يوم الأربعاء في ورشة عملنا الفنية التي نقوم بها هنا. هناك سلسلة الثقة هذه التي تذهب من هنا، والتي هي ما يسمح بالشيء الصحيح.

نقطة إضافية، حين يكون ISP - حين الدكتور إفيل - قفز هنا وقال، "هذه هي المعلومات الخاطئة" وقد رفضه، وما حصل حينها كان أن ISP قام باستفسار آخر، ووجد الخادم الصحيح، وأرجع تلك المعلومات إلى هناك. أو قد يكون قد استلم فقط استفسارين رجعا بسرعة، حسب توقيت ذلك.

حسنًا. قمنا بذلك. أعتقد أنني سأنتقل إلى روس للدخول أكثر في التفاصيل الفنية، ثم سنرجع ونحصل على وقت للأسئلة والأجوبة. لذا فكروا حول الأسئلة التي قد تريدون طرحها علينا. لدينا مجموعة رائعة من الأشخاص هنا والذين يمكنهم مساعدتنا على معالجة ذلك.

ها هو ذا، روس.

روس موندي: شكرًا لك، دان. حسنًا. أنظروا أية طريقة هنا. حسنًا. جيد. حسناً، الآن أنا لم أعد bigbank.com، لكنني روس موندي، هنا على أمل المساعدة على إعطائكم معلومات أكثر حول بعض الأجزاء الفنية من DNSSEC ولماذا يجب عليكم حتى القلق بشأن DNS للبدء به.

في الواقع، كما قمنا بهذا مع مرور الوقت، هذا الجزء - أي "لماذا يجب عليكم أن تهتموا بموضوع DNS" - للأسف أصبح أسهل لأن هناك الكثير والكثير من الهجمات التي تتم والتي تجعل DNS نقطة بداية أو أحياناً جزءاً مهماً جداً من الهجوم نفسه لأن كل تطبيق - لا يهمني أي تطبيق هو على الإنترنت؛ هناك استثناءات جد نادرة حيث لا تستخدمون DNS. بعض الأشخاص المهتمين بالتكنولوجيا وبضعة التطبيقات المهتمة بالتكنولوجيا حقاً ستستمر في استخدام عناوين IP، لكن لكل الأغراض، تستخدمون DNS للقيام بأي شيء على الإنترنت.

حينما يريد شخص ما الهجوم على تطبيق، من أين تبدأ؟ حسناً، مكان واحد يبدأون منه هو التطبيق. لكن مكاناً شائعاً جداً للبدء أيضاً هو DNS نفسه وتغيير معلومات DNS، تماماً كما رأيتم في المسرحية الهزلية نفسها، لأن ما الذي يقوم به DNS بالمعنى الأساسي؟ إنه يغير الاسم الذي يحب الأشخاص حقاً استخدامه إلى الأرقام التي تستخدمها حقاً البنية التحتية الأساسية الفنية IP لنقل البيانات عبر الشبكة.

إذن ما تحصل عليه هو أنك تصل إلى المكان الصحيح أو إلى المكان الخاطئ إذا تمت مهاجمتك مع DNS. باعتبارك مستخدمًا فليست لديك وسيلة للمعرفة. ذلك مشكل جدي للغاية. ذلك هو حقاً تهديد الخطف الذي كنا نتحدث عنه: عند حصول استبدال DNS أو هجوم خطف حيث أن المستخدم الذي يطلب المعلومات يحصل على المعلومات الخاطئة، ومهما حصل بعد ذلك، قد يكون أو لا يكون مرئياً للمستخدم. لكن غرض المهاجم عادة هو إلحاق الأذى بالمستخدم أو بالموقع الإلكتروني أو أية تسهيلات أخرى، سواء كان خادم بريد إلكتروني أو أي شيء آخر يذهب إليه.

أحد الأمور التي رأيناها من حيث كيفية الإتاحة الواسعة لأدوات اختطاف DNS. للأسف، يوجد الكثير منها، وهي متوفرة بسهولة. لا أضع الروابط في الشرائح. سيجعل ذلك سهلاً جداً للأشخاص وواسع الانتشار.

لكن في الحقيقة، في نطقة ما - وقد ذهبت المعلومات من الإنترنت لمدة - كان هناك في الواقع أستاذ جامعي وجدت دورة دراسية له بأن المشروع النهائي لهذه الدورة حول علم الحاسوب كان هو تصميم البرمجيات التي تقوم باختطاف DNS. إذن فهم يدرسون ذلك في دورة للمستوى الجامعي. بقدر ما يمكنني قوله، فقط بالنظر إلى المنهج الدراسي، فلم تكن هناك أية أخلاقيات مرتبطة به. لذا كان فقط دورة برمجة، بقدر ما يمكنني قوله. من المؤسف أن الأشخاص يقومون بذلك، لكنه موجود، وهناك الكثير من البرمجيات المتوفرة للقيام بهذا.

لذا ما الذي نحاول فعله مع DNSSEC؟ كما رأيتم في المسرحية الهزلية، كنا نحاول التأكد من حصول المستخدمين على المعلومات الصحيحة وأنهم بدورهم يمكنهم الذهاب إلى المكان المناسب الذي يريدون الوصول إليه.

هنا شريحة تعطي توضيحاً آخر لما كانت المسرحية الهزلية تظهره. هذا أيضاً نوعاً ما مختصر لأنني لم أقم بتضمين، فقط بسبب علمه، أسهم البداية في الجذر ومرورها عبر com. هذا يذهب فقط من مستخدم إلى www.bigbank.com في الواقع. إذن يذهب الاستفسار إلى خادم اسم bigbank.com ثم يعطيه ذلك الجواب من أجل www.

حين تعد الاستفسارات - أعتقد أنني قمت بعدها هناك - نعم، هناك أربعة تبادلات حزم يجب أن تحصل قبل الاتصال الفعلي للمستخدم بخادم الويب، والذي يريد المستخدم الحديث معه، على أي حال. لذا كل هذه الأمور تحصل في الخلفية التي تحصل بسرعة شديدة.

لدينا صورة هنا لموقع معد ليظهر للمستخدم إذا ما كان في الواقع DNSSEC خاصته يعمل بشكل مناسب أم لا. أحد الأمور التي قمنا بها هنا هي فقط وضع هذا كمثال خاص حتى يتمكن الأشخاص من رؤية متى يذهبون إلى هذا الموقع.

هذا، مجدداً، توضيح آخر. الدكتور إفيل هنا في الأسفل في الدائرة الصفراء الصغيرة في الأسفل، قفز هنا، وأعطى الجواب الخاطئ، وكما يمكن أن تروا على الجانب الأيمن - نعم، على الجانب الأيمن - ويرسل الأشخاص إلى المكان الخاطئ.

نعم، في هذه الحالة، لدينا مثال. هذه في الواقع لقطات شاشة أخذتها من خطف حقيقي قمنا به كإثبات في اجتماع مشابه لهذا. لم يكن اجتماع ICANN، لكنه كان اجتماعاً مشابهاً حيث جهزنا الموقع حيث، حينما كنت تستخدم DNSSEC للذهاب للموقع، ستحصل على المحتوى المناسب للموقع.

حينما يحصل خطف، ستنتهي حقاً بالحصول على جزء من الصفحة - ليس الصفحة كاملة، أو الموقع كاملاً، لكن جزء من الصفحة - مستبدل. يمكنكم رؤية ذلك، على اليسار، مع الموقع الذي عليه علامة اختيار DNSSEC - ينشر Comcast مشورة DNSSEC وما إلى ذلك - وإذا نظرتم على يمين الصورة على مستوى أسفل، فهناك قصة أمام ذلك في الواقع، حيث يعلن ستيف كروكر أن DNSSEC لن يلبي حاجات العالم. خيالي بوضوح، ومقصود أن يكون كذلك، لكن فقط من أجل التوضيح.

لذلك حينما تقوم بخطف DNS، فقد تخطف الموقع كاملاً، أو قد تخطف جزءاً صغيراً جداً ومختاراً من الموقع، ويحصل المستخدم على بقية المعلومات من الموقع نفسه، حسب كيف تم تنفيذ الاختطاف نفسه.

الصورة شبيهة لتوضيح حيث أنه، حينما تفكر في ملء تلك الصفحة التي عليها الكثير من الروابط - كان ذلك CNN.com منذ ثماني أو تسع سنوات تقريباً. وقد تحققنا من ذلك أكثر مجدداً مؤخراً. إنه أكثر ازدحاماً مما هو عليه الآن. إذن فهذا ما يأخذه، عدد استفسارات DNS التي يأخذها لملء المتصفح للصفحة الرئيسية بموقع CNN.com إذا لم يكن لديكم أي من التخزينات المؤقتة ممتلئة للبدء بها. إنها حقاً أكثر من 100 - حسناً، أكثر من 100 بكثير. إنه قريب من 200 الآن. لقد كان 70 منذ سنوات مضت.

حينما تفكر في ذلك، من الأسهل التفكير فيه كموقع كامل، لكنه حقاً ليس لأن كل موقع كبير، وكل موقع تجاري، لديه فقط عدد هائل من الروابط ومن عمليات البحث DNS. لذا يمكن أن يكون أحد أو كل تلك التي يتم خطفها.

أهمية كل هذا وكل حماية محتوى DNS هي محتوى DNS نفسه. DNSSEC مهم للغاية للمستخدمين ليكونوا قادرين على معرفة أنهم يحصلون على المحتوى الصحيح. لكنه ليس أكثر أهمية من المحتوى نفسه. وفي حقيقة الأمر، فإن المحتوى هو المفتاح الحقيقي هنا. DNSSEC موضوع في مكان لضمان أنه يمكن تحديد المحتوى الصحيح من طرف متلقي استفسارات DNS.

لذا فإن آليات التشفير التي ترون ليست أكثر أهمية من المحتوى. بعض الأشخاص يحتارون بشأن تلك الحقيقة ويعتقدون أن التشفير هو أهم شيء. إنه حقاً ليس كذلك. الأهم حقاً هو محتوى نطاقات DNS.

وهنا بعض الأمثلة القصيرة للتنفيذ. أحدها هو فقط تخطيط قياسي لكيف يتم وضع بيانات المستخدم. إنه إدخال محتواك في الخادم الرسمي لنطاق. إنه صندوق الخادم الرسمي. الخادم التكراري، الذي هو ISP - جاك في مسرحيتنا الهزلية هنا - يذهب ويطرح استفسارات عن ذلك استجابة للسيد المستخدم جو. إذن هذه طريقة أخرى فقط لتوضيح طريقة وضع المحتوى وأخذه.

ما يضيفه DNSSEC هو بعض الخطوات الإضافية القليلة التي يجب عليك القيام بها للتأكد من وضع معلومات DNS الإضافية وأنه يتم التأكد منها.

ما نقوم به هنا هو الحديث عن درجة صعوبة أو سهولة الحصول على المحتوى وتسييره تسيير DNS خاصتك أو، إذا كنت مستخدماً يسير تشغيل شركة كبيرة تضمن DNS، وما الأشياء التي يجب عليك القيام بها للتأكد من أنها موجودة.

ولن أتطرق لكل هذه الأمور بالتفصيل. نريد إبقاء بعض الوقت للأسئلة. إذا كانت هناك أسئلة، رجاء اطرحوها خلال فترة الأسئلة والأجوبة.

إذن هذه هي النطقة الأساسية التي أود طرحها بقدر ما أن جميع الأجزاء المشاركة في DNS وأمن DNS: إنه محتوى بيانات النطاق. المحتوى هو المهم. هذا ما أريد قوله. إن المحتوى هو الذي يخلق الفرق لأن عليك وضعه بشكل مناسب، وعليك تسييره بشكل مناسب، وعليك حمايته بشكل مناسب مع DNSSEC.

في هذه الحالة، إنها نفس مجموعة الصناديق. أسهل تنفيذ هو توقيع نطاق - أليس لدينا أي مؤشر؟ على أي، البيانات الموقعة يتم وضعها في الخادم الرسمي، ويقوم الخادم التكراري بالتحقق. التنفيذ الأبسط الذي لديك، هو ذلك المفتاحان في الواقع، القضايا البالغة الأهمية. يتم توقيع بيانات النطاق والذي يتم وضع البيانات فيه، ثم يتم التحقق منه من طرف محلل تحقق عند حصولك على البيانات. هذه أبسط وأسهل طريقة لوضع DNSSEC خاصتك.

من حيث ما يمكن للمستخدمين القيام به بشأن التنفيذ وخصوصاً لمنظماتهم، مهما تكن تلك المنظمة - إذا كان لديك نشاط كبير حيث تركز الشركة بشكل كبير على DNS (مرتكزة على DNS)، فهناك احتمال كبير أن لديك بالفعل طاقم DNS مؤهل بشكل كبير ومختص. المنظمات مثل ذلك يمكنها عادة أخذ DNSSEC وتنفيذه لأنفسهم. مهما كانت الأجزاء، فيمكنهم عادة القيام به لأنفسهم.

وإذا كنتم منظمة تقوم بتعهيد الكثير من دعم DNS لديها، فسترغبون في الذهاب إلى أولئك الذين تطلبون منهم الدعم وستطلبون منهم القيام بتنفيذ DNSSEC لأجزاء DNS التي يشغلونها لكم.

إذا لم يقوموا بذلك، فعليكم اعتبار إيجاد شخص ما يقوم بذلك لأنه لا يوجد شيء يجعل الشركات تتحرك بشكل أسرع من احتمال فقدان عملاء. هذا شيء مهم. اطلب من موردك إذا كنت تقوم بالأمر بنفسك. واطلب من موفري الخدمات إذا كان لديك من يقدم لك الخدمة. اطلب دعم DNSSEC. تلك ربما أكبر رسالة لما يمكن لأي أحد القيام به: أطلب من أولئك الذين يقومون بأمور DNS لهم، "هل لديكم DNSSEC، وإذا لم يكن لديكم، متى ستحصلون عليه؟ لأنني أريده وأريده الآن."

حان وقت الأسئلة. سيكون لدى دان وأنا عادة الميكروفونات، لكن لدينا مجموعة من الخبراء هنا. جولي؟

جولي هيدلوند: [غير مسموع]

روس موندي: أوه. بالنسبة للميكروفون الذي يشتغل، بالطبع. نعم.

دان يورك: لدينا حوالي نصف ساعة أو ما شابه. لدينا الكثير من الوقت. ما رأيكم، إذن؟ هل لديكم أية أسئلة؟ أليس كذلك؟ سأجع إليك، أظن، لأنه ليس لدينا حامل ميكروفون. ها هو ذا، إنه جيد. يمكننا الجري هنا، والقيام ببعض التمارين الرياضية.

جاك لاتور: ويمكنهم طرح الأسئلة بالفرنسية، وسأترجم.

سيدة غير معروفة: شكرًا. [غير مسموع] لأوغندا. سؤالي حول اسم النطاق - نعم، الأمن، ولقد قلت لنا للتو. بقيت أتساءل. أحد طرق تأمين اسم نطاق هو عبر استخدام شهادات SSL، أليس كذلك؟ لكن كيف يتم في بلدي، وأغلب أسماء النطاقات الحكومية، يتم اختراقها؟ وكيف [غير مسموع] شهادات SSL؟

دان يورك: فلنأخذ ذلك جزئياً بمجموعة من الطرق المختلفة. سؤال ممتاز لأن الأشخاص يطرحون ذلك السؤال. أحد الأسئلة التي يطرحون هي، "لدي شهادة TLS (أو SSL)، وأنا محمي، إذن يجب أن أكون آمناً."

حسناً، هناك مجموعة من الأمور المختلفة التي تحصل. أولاً وقبل كل شيء، رأيت هنا أن مجالاً للتعرض هو هذا، الوصول إلى عنوان IP الخاطئ. إذن أحد المجالات هو خطف DNS. يمكن أن يحميك DNSSEC من ذلك التهديد الخاص.

لكن الآن تصل إلى، في المستوى الأعلى، الأسئلة بشأن أية شهادة TLS يجب استخدامها. هل هي الشهادة الصحيحة؟ لدينا جزء آخر من DNSSEC. هناك شيء يسمى DANE - بروتوكول DANE - والذي يسمح لك بوضع شهادة TLS في DNS، وتسجيلها مع DNSSEC، وكيف أنه حين يذهب شخص إلى موقعك، يمكنه تشفيرياً معرفة أن تلك هي شهادة TLS الصحيحة للاستخدام.

مع قول ذلك، بالطبع معظم بائعي المتصفحات لم ينفذوا ذلك بعد. إنه أمر أحدث بطرق معينة حول ذلك. لكنه يتم استخدامه في البريد وبعض الأماكن الأخرى.

بخصوص لماذا يتم اختراق تلك المواقع، فإن هناك مجموعة كاملة من القضايا التي تدخل في المواقع والتي تحصل في الواقع على مستوى أعلى، أي على مستوى التطبيقات. في كثير من الأحيان تكون لمواقعهم مشاكل في أشكال، مثلاً، سيسمح ذلك للأشخاص بخطف المواقع عبر ذلك، أو طرق أخرى للدخول في تلك الخوادم التي لا تدخل [غير مسموع] TLS لأن TLS يشفر الصلة بين المتصفح والخادم. لذلك فإنه يوفر الحماية هناك. DNSSEC يوفر الحماية هناك، لكنه لا يقوم بأي شيء لحماية ما يقوم به الأشخاص داخل الموقع. إنه فقط يقوم بنفق آمن، أساساً، بين المتصفح وذلك. لذلك يمكنهم القيام بجميع أنواع الأمور داخل هناك، ويمكنهم الاختراق هناك وطرق أخرى - أوه.

روس موندي: إذا ما نظرتم إلى الأسهم هنا، تشير الأسهم الحمراء إلى استفسارات DNS، والأسهم الخضراء هي في الواقع استفسار HTTP/HTTPS بين المتصفح وخادم الويب. ما يقوم به DNSSEC هو ضمان أنك ستصل إلى خادم الويب الصحيح.

الآن، إذا تعرض خادم الويب نفسه لهجوم ناجح، فذلك أمر لا يستطيع DNSSEC أن يفعل أي شيء حياله. أو إذا، في الحقيقة، إذا كان مرجع شهادة TLS مخترقاً وقام أحد بشيء بسبب اختراق ذلك المرجع للشهادة، فذلك خارج ما يستطيع DNSSEC القيام به. لذا وقتما ذهبت إلى موقع يقوم بوظيفة من نوع تطبيق، فإن ذلك الموقع لا يزال عليه الاشتغال والقيام بالموظيفة بشكل صحيح. يضمن DNSSEC من وصولك إلى الموقع الصحيح، لكن لا يضمن أن يعمل بشكل صحيح لصالحك.

سيدة غير معروفة: حسنًا.

روس موندي: هل هذا مفيد؟

سيدة غير معروفة: إذن [غير مسموع] غير مضمون -

دان يورك: لا. يضمن DNSSEC فقط أنك تصل إلى عناوين IP الصحيحة. ويضمن TLS أنك تحصل على اتصال مشفر بين العميل والخادم. لكنهم حقاً فقط يحمون الاتصال للوصول إلى هناك. ما الذي يحصل حقاً للخادم، أو لمتصفح الويب؟ إذا كان لدى شخص ما برنامج مؤذ أو شيء على خادمه، أو على حاسبه المحمول أو أي شيء، فإن ذلك فقط يحمي النقل والاتصال. DNSSEC بالخصوص يقوم بتلك العناوين IP وعملية البحث تلك.

هناك مجموعة كاملة من الأمور الأخرى التي يمكن أن تسبب مشاكل للخوادم.

سيدة غير معروفة: حسنًا.

دان يورك: تعليقات أو أسئلة أخرى؟ موجود هناك. تريد كاثي القيام بالجري الآن.

كاثي سكنيت: كان علي أن أنتعل المزلجة ذات العجلات.

دان يورك: أعرف ذلك. المزلجة ذات العجلات. لا بأس بهذا. وإذا أراد أي أحد آخر منكم أن يقتحم هنا أيضاً، فروس وأنا ليس علينا أن نتحدث.

جاك لاتور: ذلك إذا ما سمحتم لنا.

دان يورك: ماذا؟ أوه، ذلك إذا ما سمحنا لكم. عذرًا. تفضل.

شخص غير محدد: انطلاقاً من المبيانات والمسرحية الهزلية، يبدو أن DNSSEC يحتاج أن يتم تنفيذه من أطراف متعددين. إذن موفر ISP يجب أن يدعمه. ومنطقة الجذر يجب أن تدعمه. والسجل يجب أن يدعمه، وكل موقع يجب أن يدعمه. هل هذا...

دان يورك: حسناً...

شخص غير محدد: أو يجب على أن أقول كل اسم نطاق.

دان يورك: كل اسم نطاق، نعم. هناك مجموعة من الأماكن هناك. مجدداً، هناك جانبان. هناك جانب التقييم، والذي هو التحقق، والذي يجب على ISPs ومشغلو الشبكات القيام به.

وذلك حقاً من السهل القيام به. يمكنك عبر BIND، أو Unbound، أو Windows Server. أي من هذه الأمور التي تقوم بتحليل DNC تدعم الآن تحقق DNSSEC. لذا يمكنكم الذهاب إلى شبكاتكم اليوم وتشغيل ذلك.

هناك تحذير أنكم تحتاجون أن تكونوا واعين بذلك، إذا كان لشخص توقيع سيء أو شيء ما، فقد توقفون الأشخاص من الذهاب من هناك. لذا عليكم أن تكونوا حذرين بأن، تشغيله، قد تبدأ حماية الأشخاص، لكن ذلك قد يسبب بعض، إذا كانت هناك مشاكل هناك. ذلك هو جانب التحقق.

جانب التوقيع ينطوي على - نعم، تم توقيع الجذر في 2010. أغلب TLDs العامة وكل TLDs العامة الجديدة تم توقيعها كلها في مستواهم الأعلى. الكثير من رموز الدول - ccTLDs - تم توقيعها، رغم أن إفريقيا، الكثير منهم هنا، هم الذين ينقصهم ذلك التوقيع على المستوى الأعلى. لقد كنا نعمل للمساعدة في ذلك. لكنكم تحتاجون ذلك. ثم يحتاج أمين السجل خاصتكم دعمه كذلك لأن عليهم تمرير جزء ذلك التوقيع الصغير للقيام بذلك العمل.

إذن فجانب التحقق بسيط نسبياً. جانب التوقيع؟ هل تحتاج الحصول على أولئك الممثلين الثلاثة هناك.

يود وارين قول شيء ما - أوه، تريد جولي قول شيء.

جولي هيدلوند: أجل. أريد فقط تذكير الأشخاص، عند طرح الأسئلة، رجاء اذكروا أسماءكم ورجاء أيضاً اذكروا من تمثلون. شكرًا.

[شخص غير محدد]: أجل. بشأن ISP أو من جانب التحقق، حالياً حوالي 20% من استفسارات DNS تمر عبر محلل تحقق. إذن هناك على الأقل بعض النشر من هذا الجانب. إنه ليس حقاً بالمستوى الذي نريده، لكن 20% أيضاً رقم جيد.

دان يورك: صحيح. وبعض المواقع الكبرى، مثل خادم DNS العام لشركة Google، تقوم بتحقق DNSSEC بشكل افتراضي، لذا إي شخص يستخدم 8.8.8.8 و [غير مسموع] عناوين IPv6، فإن كل ذلك يتم التحقق منه بشكل افتراضي.

هيث ديكسون: حسنًا. أنا هيث ديكسون من شركة Amazon. سؤال آخر. ذكرت أمين السجل كذلك. لذا هل هو أمين السجل أو اسم النطاق، أو كلاهما؟

دان يورك: أنت كمالك اسم نطاق قد لا يكون عليك القيام بالكثير، لكن هناك شخصاً يقوم بخدمة تسجيلات DNS؛ لذا فإن مشغل استضافة DNS، كما نسميه عادة، أو مشغل DNS، والذي هو في حالات كثيرة أيضاً هو أمين السجل. لكن لا يجب أن يكون كذلك.

أنتم مشغلو DNS، لذا فأنتم تخدمون المناطق الأخرى. عليكم أن توقعوا المناطق لأن كل تسجيل زمني يتم تغييره في DNS، يجب أن يكون له توقيعات جديدة، أو مجموعات التسجيلات تحتاج توقيعات جديدة.

حسنًا. جاك يود أن يجيب. لكن المفتاح هو، أن المشغلين عليهم أن يوقعوه، ثم أمناء السجلات - وأعلم ما يقوم به جاك؛ حسناً - ثم على أمين السجل أن يحصل على تلك المعلومات لتمريرها إلى السجل.

لدي مشكل مع أحد نطاقاتي وهو أن أمين السجل لا يدعم DNS - لا يسمحون لي بوضع التسجيلات هناك. لذا أنا حقاً أنتقل إلى أمين سجل آخر يدعم DNSSEC.

لكن جاك يريد أن يقول لكم عن هذا الأمر الخاص، على ما أعتقد.

جاك لاتور: نعم. إذن قلت أنت مع Amazon، أليس كذلك؟ أظن أن بعض كبار DNS يوفرون مشغل DNS. يمكنهم توقيع منطقتهم لأنفسهم أو لعملائهم، والتحدي هو جعل تسجيل DNS يوقع المنطقة عبر أمين السجل الصحيح إلى السجل الصحيح.

ما نقوم به الآن هو أننا نبني نوعاً جديداً من الواجهة لمشغلي DNS للتوقيع الذاتي لنطاقاتهم دون أمين سجل، أو مع أمين سجل. نحن نعمل على طريقة جديدة لجعل تمهيد التوقيع على أسماء النطاقات أسهل لمعالجة بعض قضايا مشغل DNS.

دان يورك: سيرغب جاك في التحدث إليك بعد هذه الجلسة.

روس موندي: شكراً لك على ذلك السؤال. أود أيضاً أن أضيف أنه في الحقيقة فإن حامل الاسم، سواء كان يشغل أياً من خدمات DNS المرتبطة بالاسم أو لا، يجب أن يكون من يبدأ حقاً، أو إذا ما أردتم، يتخذ القرار: "أريد الحصول على هذا الاسم موقعاً DNSSEC."

تفاصيل ما يجب أن يحصل بعد ذلك تختلف حسب أية خصوصيات للعملية. الكثير منا سيكون سعيداً للذهاب إلى أي مستوى من التفاصيل لأي سؤال يكون لديكم بعد هذا، لكنني أتخيل أنكم تشغلون الخوادم الرسمية المحللة DNS الخاصة بكم لشركتكم. لذا سيكون ظني أن التحدي قد يكون هو الحصول على تسجيل DNS في السجل. هناك أجوبة لكيف يمكن القيام بذلك.

هيث ديكسون: شكرًا.

دان يورك: إذا لم تدركوا، أي منا قد يدخل عميقاً إلى حفر الأرانب في وصف هذا النوع من الأمور. لذا إذا أردتم الحصول على مناقشة فنية عميقة، فسنكون سعداء بذلك.

هل ثمة أحد آخر؟ هيا، شخص آخر. لدينا هذه المجموعة من الأشخاص هنا. يريدون الإجابة عن الأمور.

عادل صادق: معكم عادل صادق من باكستان. أنا مشارك من NextGen. بالإشارة إلى دورك، لدي سؤالان من دورك. حينما كان البنك يحول السلسلة من البنك إلى المستخدم جو، لماذا لم يتمكن الدكتور إفيل من القيام بهجوم رجل-في-الوسط هناك. السؤال الأول.

سؤال ثاني. لماذا أنتج الدكتور إفيل تلك السلسلة من المصادقة باستخدام IP البنك، حتى قبل بدء البنك تلك العملية؟

دان يورك: هل يرغب أي شخص في اللجنة الإجابة على ذلك لأنه تم اتهامي -

ويس هيرداكر: بالحديث بصفتي جو، أستطيع الإجابة على ذلك.

دان يورك: حسنًا.

ويس هيرداكر: طرحت بضعة أسئلة. دعني أتطرق للسؤال الأول أولاً. هناك مشكل بين المستخدم جو و ISP خاصته. لاحظ أن ذلك الاتصال لك تتم المصادقة عليه. الحل لذلك هو أنه يمكنك في الواقع تشغيل محلل تحقق على جهازك الموضعي. أشغل واحداً على حاسبي المحمول. إنها صغيرة بما يكفي وخفيفة الوزن بما يكفي حتى أني جمعت واحداً وأشغله على هاتف. ليست صعبة جداً لوضعها على جهاز صغير. هذا ريما من المحتمل أكثر أن يكون خطوة مستقبلية. والبعض منا يقوم بذلك الآن بالفعل.

هناك برنامج يسمى DNSTrigger والذي سيقوم في الواقع بذلك لك نوعاً ما بشكل آلي. سأحاول القيام به حين يستطيع. إذا كنت في فندق حيث لا يعمل ذلك، والذي هو للأسف أمر يقع، فإنه يفشل مجدداً في استخدام DNS العادي. إذن هناك حلول لذلك قادمة.

سأتوقف عن الجزء الثاني من سؤالك لأنني سافرت للتو منذ ساعة من مسافة بعيدة جداً.

[شخص غير محدد]: لماذا لا يستطيع الدكتور إفيل أن يزيف الجواب؟

دان يورك: بين Big Bank و -

ويس هيرداكر: إذا تذكرتم حقاً بسرعة، في المسرحية الهزلية، كل الممثلين تبادلوا توقيعاً في وقت مبكر، لذا فقد اتفقوا قبل الوقت. عندما تسجل في أمين السجل خاصتك، مثلاً، وتسجل في نطاق جديد لنطاق example.com، يجب عليك أن يقول لأمين السجل أنك تحتاج تسجيلاً خاصاً موضوعاً في com الذي يصادق على تسجيلاتك في example.com. إذن ذلك حقاً مرتبط بشدة والدكتور إفيل لا يمكنه إدخال شيء في أي مكان.

لذلك ليس فقط في النهاية يمكنه أن يكون قد حاول ذلك الهجوم. في أي مكان على الخط، من الجذر أسفل لمحلل example.com سيتجنب ذلك الهجوم. هل يبدو ذلك منطقيًا؟ أرجو ذلك.

دان يورك: جاك، هل أردت قول شيء - أوه، حسناً. لقد قمت بذلك. أجل. لأنه كان يمكن أن يأتي الدكتور إفيل مع حزمة عليها توقيع. يمكنه القيام بذلك. لكن مجدداً، إنها سلسلة الثقة تلك، هذه السلسلة العالمية للثقة بين الجذر إلى TLD إلى نطاق المستوى الثاني، إلى آخره. هذا يضمن ذلك، حتى إذا أتى الدكتور إفيل مع ذلك التوقيع، فسيقول ISP، "حسناً، لديك توقيع، لكنه ليس التوقيع الصحيح. إنه لا يتابع كل الطريق للعودة إلى الجذر."

شخص آخر ويس قال بقدر ما - كان يمكن للدكتور إفيل أن ينقض بين ISP والمستخدم جو. هناك في الواقع فريق عمل داخل فريق عمل هندسة الإنترنت، IETF، المسمى Deprive، حيث وارين كان يقفز لأنه الرئيس المشارك له هناك، والذي يعمل على كيف تؤمن ذلك الاتصال بين المستخدم جو و ISP لنظام DNS حتى يمكنكم الانتهاء بالحصول على اتصال آمن هناك حتى لا يتمكن الدكتور إفيل من الانقضاض بين ISP وذلك. إذن تلك طريقة واحدة.

الطريقة الأخرى هي، كما قال وس، بدأ المستخدم جو تشغيل محلله للتحقق وقام فقط بذلك بنفسه بطريقة أخرى.

أية أسئلة أخرى؟ هناك. نعم.

هبة التيجاني: هبة التيجاني، زميلة في ICANN. أريد فقط بعض المعلومات الموجزة حول عملية التوقيع والتحقق؛ حيث يتم تخزين الشهادات، كيف نقوم بالتحقق، والأمور مثل ذلك.

دان يورك: بالتأكيد. أي شخص آخر قبل - حسناً. إذا أردت.

ويس هيرداكر: حينما توقع منطقة، عليك تخزين المفاتيح على جهازك. هناك في الواقع وثيقة كاملة حول أفضل الممارسات حول كيفية القيام بذلك. يمكنكم إلقاء نظرة عليها. إنها RFC. لا أعرف الرقم على أعلى رأسي. لكنه يجب عليك تخزين الاثنين الشهادة والمفاتيح، ثم ما تضعه في الواقع في DNS هو فقط الجزء العام. إذن تضعون المفتاح العام وسيضع مزودك رابطاً لذلك المفتاح العام في تسجيل خاص يسمى تسجيل DS. المفتاح الخاص الذي تخزن على جهازك، أو ربما على جهازك المستقل، لأنك لا تحتاج المفتاح الخاص على الإنترنت. تم تصميم DNSSEC بحذر شديد حتى تتمكن من الحفاظ على المفاتيح الخاصة في قنطرة جد خاصة وفقط وضعه حين تحتاج توقيع المنطقة. لا يجب أبداً أن يتم تعريضه للإنترنت الحقيقي. هليك فقط تحويل التسجيلات الموقعة والمفاتيح العامة إلى DNS الحقيقي.

يحتفظ بعض الأشخاص بمفاتيحهم الخاصة على الإنترنت إذا كانوا يحدثون بسرعة، وإذا كانوا يغيرون الأمور كثيراً، أو إذا كانوا يحاولون القيام بتحديثات مباشرة لنطاق DNS الديناميكي والأمور الأخرى. لكن لست مضطرًا لذلك.

دان يورك: وهناك ما يسمى بيانات ممارسة DNS، أو وثائق DPS، المتاحة من كل TLDs والتي تشرح ما يقومون به.

الآن، البعض مثل منطقة الجذر لديهم عملية جد قوية تمر عبر تفاصيل دقيقة لحماية المفاتيح الخاصة والتأكد من جميع الأعمال. لدينا أشخاص هنا شاركوا في ذلك، وذهبوا في قناطر وكل أنواع تلك الأمور المختلفة.

حسنًا. لكن بالنسبة لكثير من TLDs الأخرى، يستخدمون آليات أخرى هناك. بالنسبة لنطاقات أخرى، بالنسبة لنطاق فردي، قد يقوم المشغل به ويحتفظ به جميعاً في أنظمتهم الخاصة بطريقة ما. لذلك فالكل يعتمد حقاً على مستوى الخطر الذي تريد الحصول عليه في ذلك.

الآن، من جانب التحقق، أنت حقاً فقط داخل برمجيتك التي تشتغل على خوادمنا. عادة على ISP، قد يشتغل على محللي DNS التي توجد في حدود الشبكة.

هذه الأيام، إنه سهل مثل تغيير تعليق لخط في ملف إعداد يقول، "شغل محلل DNSSEC،" وهذا كل ما في الأمر. الآن سيبدأ في القيام بتحقق DNSSEC كل الوقت. BIND، أو Unbound: لقد جعلوا ذلك كله بسيطاً جداً لإزالة علامة التعليق فقط والآن تعملون.

بعض الأمور الأخرى التي قد تكون خطوة أخرى أو اثنتين هناك، لكن من السهل جداً تمكين ذلك. ثم يبدأون لك التحقق لكل استفسار DNS يحصلون عليه.

روس موندي: أيضاً، أود الإشارة إلى أن الكثير من الأشخاص ينظرون إلى أن ما يعتقدونه الوظيفة الأكثر أهمية للأمن سيتم ربطه مع DNS الذي يشغلون.

كما قال دان، لدى الجذر حجم كبير من هيكل الأمن حوله. يستخدمون ما يسمى نماذج أمن المعدات. الكثير من TLDs أيضاً يستخدمون نماذج أمن المعدات حتى تكون الطريقة الوحيدة لإعادة توقيع منطقة على المستوى الأكثر حساسية لإعادة توقيع منطقة هو لجلب تلك النماذج لأمن المعدات من الأمن، والمرور عبر عملية كبيرة، والحصول على شهود. الكثير من العمل الشاق.

أشخاص آخرون ينظرون ويقولون، "ما هو محتوى منطقتي لا يتم استخدامه بحساسية." حسناً؟ الشركة التي أعمل لصالحها هي parsons.com. حينما تم توقيع parsons.com، ذهبوا مع مزود خارجي لأنه كانت لديهم بالفعل عمليات معدة. إذن كل نشاط فردي يحتاج أن يعتبر كيف هي حساسة الأمور التي تحصل مع DNS خاصتهم.

إذن ذلك طيف لكيف تتعامل مع مفاتيحك وشهاداتك، لكن يجب أن يتم النظر إليه فردياً لكل نشاط ثم اتخاذ القرار. لكن هناك الكثير من المساعدة المتوفرة، والكثير منها مجاني، لأن هناك الكثير من الأمثلة على الإنترنت. وهناك الكثير من الممارسات التي كتبها الأشخاص ونشروا علناً. إذن هناك الكثير من الأمور التي تمكنك من الحصول على المعلومات التي ستساعدك حين تتخذ تلك القرارات الخاصة لأنه، تذكر، إنه المحتوى وما يتم استخدام المحتوى لأجله. ذلك ما يهم.

دان يورك: جاك يريد التدخل. أود فقط أن أقول، كمستخدم فردي، وقعت على مجموعة من نطاقاتي - أوه، تفضل، جاك، أولاً.

جاك لاتور: الجواب البسيط هو، إذا استخدمت برمجية تجارية تدعم DNSSEC، إضغط على نعم، وفي الغالب سيقوم بذلك بشكل صحيح.

دان يورك: حسناً، سأقول، بالنسبة لبعض النطاقات، مشغلو DNS الذين أستخدمهم، أحدهم قام به حيث كل ما أقوم به هو التحقق من صندوق يقول "تمكين DNSSEC،" ويهتمون بكل شيء لي.

في آخر، كان علي الذهاب إلى مجموعة أخرى من علامات التبويب لإيجاد أمر DNSSEC. ثم ذهبت هناك وضغطت على هذا وقلت "افعل DNSSEC الآن،" وكان ذلك كل ما كان علي القيام به. إنهم فقط يهتمون بتغيير المفاتيح لي، ويقومون ببعض ذلك كله آلياً.

الآن، يحدثت أيضاً عن التحقق. صديقي، بول ووترز هنا، الذي يلبس قبعة حمراء، أشار إلي أن BIND الجديد، أو Unbound الجديد، النسخ الأحدث منها، لديها تحقق DNSSEC ممكن افتراضياً. لذا بمجرد تثبيتها، فإنها تقوم آلياً بتحقق DNSSEC.

شكرًا لك، بول. وارن رفع يده هناك.

وارن كوماري: أجل. هناك عدد كبير من موفري DNS وموفري CD الذين هم بالفعل أو سيفعلون قريباً آلياً DNSSEC للجميع. إذن هذا يتحرك. إذا لم تركب في السفينة الآن، فستغادر بدونك.

دان يورك: يوم الأربعاء - سأضع مكوناً جديداً - هناك ورشة عمل DNSSEC يحصل من 9:00 صباحاً إلى 2:15 مساءً. وهناك جدول أعمال يمكنكم الاطلاع عليه على الإنترنت. هناك حقاً جلسة كاملة حول الدخول إلى بعض وحدات البرمجيات وبعض أجزاء توقيع البرمجيات، إلى آخره، والتي ستعمل هناك.

ستكون لدينا مناقشة من أحدهم، وهو CloudFlare. أحد المشغلين سيكون هناك يتكلم عن عملهم على توقيع عدد هائل من النطاقات بنطاق واسع.

أليس كذلك؟

سيدة غير معروفة: [غير مسموع] من موريشيوس. لذا نحن نتحدث عن المفاتيح، صحيح؟

دان يورك: نعم.

سيدة غير معروفة: هل لديهم أجل انتهاء صلاحية؟

دان يورك: نعم.

سيدة غير معروفة: ما هو طول صلاحية المفاتيح، وما الذي يحصل حينما تنتهي صلاحيتها؟ شكرًا.

دان يورك: حسناً، سنجيب عن السؤال الثاني أولاً. إذا فكرت في حقيقة أنه إذا كانوا يتحققون من التوقيعات وتوقف التوقيع فجأة عن كونه صالحاً، ماذا تعتقدون أنه سيحصل؟

نعم، محلل التحقق سيقول هذا خاطئ ولن يمكنك الوصول إلى هناك.

اسمحوا لنا أن نحكي لكم قصة صغيرة. منذ سنة ونصف من الآن، إذا كانت ذاكرتي تعمل، NASA في الولايات المتحدة الأمريكية، nasa.gov، وكالة الفضاء، وقعوا نطاقهم. كان كل شيء يعمل بشكل جيد جداً. Comcast مشغل كبير في الولايات المتحدة الأمريكية. شغلوا تحقق DNSSEC لعملائهم 20 مليون في الولايات المتحدة الأمريكية. كل العملاء كان لديهم تحقق DNSSEC.

كان كل شيء رائعًا. كل الأمور كانت تعمل معاً. ثم حصل للأشخاص في NASA خطأ صغير. لم ينتبه شخص ما حقاً لتاريخ الانتهاء المضبوط له. هناك عملية محددة. عادة بالنسبة لمفتاح تقوم بها لسنة. هناك عملية أوسع. هناك مفاتيح توقيع المفتاح ومفاتيح توقيع المنطقة وأمور تصل إليها. لكن لنقل أن المفتاح الكبير الذي يجب أن تقلق بشأنه هو لسنة.

إذن NASA، شخص ما لم ينتبه تماماً، ولم يعمل تماماً، وانتهت صلاحية المفتاح. حسناً، فجأة، كل شخص كان على شبكة Comcast - وهذا كان في الواقع قبل قيام Google بهذا؛ كان ليكون أسوأ حتى اليوم - لم يتمكن من الدخول على موقع NASA. حسنًا؟ لم يتمكنوا من الدخول هناك. لم يتمكنوا من رؤية أي شيء. لا صور فضاء، ولا شيء.

الآن، المشكل بالطبع كان هو أن الجميع كان بإمكانهم سحب هواتفهم المحمولة. يمكنهم النظر هنا، ولأن هذا كان شبكة مختلفة لم تكن تقوم بتحقق DNSSEC، يمكنهم الدخول على موقع NASA على هاتفهم المحمول. إذن فجأة - أوه، وهناك عامل آخر. حصل هذا في اليوم - هل تتذكرون متى كان هناك انقطاع كبير عبر الكثير من الويب بسبب تشريع SOPA/PIPA الذي كان يحصل في الولايات المتحدة الأمريكية؟

أرى الكثير من الأشخاص يشيرون بالموافقة. كان هناك الكثير من المواقع الإلكترونية التي كانت ستتوقف ذلك اليوم احتجاجاً على قيام الحكومة الأمريكية بتلك الأمور.

انتهت صلاحية مفتاح NASA ذلك اليوم. وفجأة، يستطيع الأشخاص الوصول إلى موقع NASA على هواتفهم المحمولة. في حين لا يمكنهم الوصول إليه هنا. "لا بد وأن Comcast حجب NASA!" حسناً؟ "هذا أمر سيء." حصل غضب عارم على شبكات التواصل الاجتماعي. اجتاحت العاصفة Twitter أولاً ثم الآخرين، حسناً. كان أشخاص خدمة العملاء المساكين في Comcast فقط مثل، "ما الذي يحصل؟" بسبب كل ما كان يحصل هنا.

الآن، تم حله. حسناً؟ منذ ذلك الوقت، وضعنا تدابير وكان للأشخاص مناقشات كثيرة. كان الأشخاص من NASA رائعين لأنهم عملوا مع Comcast لتوثيق ما حصل والوصول لبعض الأمور. وقد قدموا عرضاً في أحد ورش عملنا. ذلك ربما منذ أكثر من سنة ونصف. ربما منذ سنتين أو مثل ذلك.

ماذا؟

متحدث غير محدد: 2012.

دان يورك: حسنًا. 2012. منذ ثلاث سنوات. حسنًا. حسنًا. أطول قليلاً لأننا كنا نقوم بهذا منذ مدة طويلة. على أي، الجواب هو، إذا لم تقم بذلك بشكل صحيح، فقد يسبب هذا النوع من الانقطاع وهذا النوع من الأمور.

الآن، الأخبار الجيدة هي أن هناك أنظمة موجودة الآن تجعل هذا آلياً. وهناك أفضل ممارسات موصوفة بشكل جيد. هناك أجزاء ستقوم بذلك.

أي شخص هنا من كينيا؟ حسنًا. كان في كينيا مشكلة مع هذا فقط خلال السنة الماضية.

متحدث غير محدد: [غير مسموع]

دان يورك: أجل. حسنًا. 2014. إذن السنة الماضية، أو ما شابه. في هذا الوقت، كان لدى كينيا مشكل مع هذا، أيضاً. كان لديهم أحد انتهاءات الصلاحية على TLD خاصتهم على ke. فجأة انقطعت سلسلة الثقة لأن TLD فجأة أصبح لديه توقيع خاطئ. إذن جميع من كان موقعاً تحت ذلك، جيد. رائع. ثم حينما ذهب المحللون لمحاولة تتبع تلك السلسلة، وصلوا إلى ke. و ke. كان خاطئاً، ولذا لم تعمل السلسلة.

إذن، نعم، عليك التأكد من أنه حينما تنتهي صلاحية المفاتيح - إذن التوقيع ليس فقط مسألة بسيطة من نوع "حسناً. لقد انتهيت." عليك الانتباه لحقيقة أنه، في فترة من الزمن، عليك إعادة القيام بذلك.

الآن، بالرجوع إلى نقطة جاك، كعميل، بالنسبة لي، الأشخاص الذين أدفع لهم لاستضافة نطاقي، أتحقق من صندوقي. يهتمون بذلك كله لي. لذا لا يجب علي القيام بأي شيء. لكن إذا كنت مكانهم، سيتوجب علي الانتباه لضمان أن مراحل المفاتيح تلك تعمل بشكل جيد.

شخص غير محدد: [غير مسموع]

دان يورك: ماذا؟

شخص غير محدد: الأتمتة والأدوات.

دان يورك: الأتمتة والأدوات. الكثير من ذلك حقق تقدماً كبيراً. هناك مشروع أدوات DNSSEC، والذي هو خلف بعض أولئك، والذين لديهم تلك الأدوات. الأجزاء الأخرى التي تحصل كذلك.

أعتقد أن لدينا الوقت ربما لسؤال إضافي أو ما شابه - أوه، لدينا 15 دقيقة إضافية. حسنًا. إذن هل هناك أية أسئلة أخرى؟ نعم، هناك في الخلف؟ عفوًا. سأحصل عليه.

سيدة غير معروفة: [غير مسموع] من أوغندا. فقط أسأل عمن يهتم بتلك التوقيعات؟ هل هو مراقب خادم اسم النطاق، أو مالك اسم النطاق؟

دان يورك: إنه من يوفر خدمة DNS. حامل اسم النطاق، أو مالك اسم النطاق - شخص هناك، بعض خوادم DNS، توفر هذه المعلومات. روس في تلك الصورة كان يفعل BigBank، لذا كان يوفر المعلومات إلى BigBank. إذن قام بالتوقيعات.

أنت كمالك، إذا كنت حامل النطاق، فقد رتبت معه للقيام بذلك.

الآن، يمكنك القيام به لنفسك. السيد هناك من Amazon يشغب خوادمه الخاصة، لذا سيقوم بذلك لنفسه. أنت وفريقك الفني أو أياً كان يمكن أن يشغل خوادمه الخاصة والقيام بذلك.

إنه أي شخص يشغل الخوادم.

هل يود أي شخص آخر أن يتدخل؟ لديكم دقائق إضافية قليلة. هيا. يمكننا تلقي الأسئلة بالفرنسية، كذلك. لقد تعلمنا ذلك. إذا كانت لديكم أسئلة بالفرنسية، السيد جاك سيترجمها لنا، لذا لا تقلقوا بشأن ذلك.

وارن كوماري: أجل. رجاء اطرحوا سؤالاً بالفرنسية. سيكون من الممتع رؤية دان يحاول تصور ما يعني ذلك.

دان يورك: الآن تذكروا، إنه فرنسي كندي، لذا فلغته الفرنسية لن تكون مشابهة للغتكم. حسنًا. ها نحن ذا.

جاك لاتور: سؤال باللغة الفرنسية؟ [غير مسموع]

شخص غير محدد: لأني أتقن الفرنسية، أنا [غير مسموع] الآن. أود معرفة أنه بما أنكم قررتم أن التوقيع كان لعملية الحل، فلا أفهم إذن لماذا، ما هو الدور الذي يلعبه أمين السجل. ما هو دور أمين السجل؟ اشرحوا لي ما هو، عملية التوقيع، دور أمين السجل.

جاك لاتور: ليس لأمناء السجلات دور جد مهم في DNSSEC. ليست هناك قيمة مضافة لأمناء السجلات في DNSSEC. هذا هو المشكل الذي لدينا في كندا بشأن ca. لدينا 180 نطاقاً موقعاً، والسبب لذلك هو أن أمين سجل واحد من بين 180 يدعم DNSSEC. إنهم ليسوا مهتمين. إنها تكلفة مضافة لعملياتهم. إنه باهظ للغاية.

إذن نحن نبحث عن طريقة جيدة لتوقيع اسم نطاق دون استخدام أمين السجل. يوم الأربعاء خلال ورشة عمل DNSSEC، إذا أتيتم سنتحدث عن ذلك.

دان يورك: حسنًا. المتحدثون بالألمانية، يمكنني مساعدتكم هنا، لكن - أوه، ها نحن ذا.

شخص غير محدد: سوف أتحدث باللغة الفرنسية. أنا من مالي. هل تنشر ICANN اليوم لائحة لأمناء السجلات الذين يدعمون DNSSEC لنطاقات gTLDs؟

جاك لاتور: بخصوص gTLDs الجديدة، من الإلزامي دعم DNSSEC. بالنسبة لأمناء السجلات، DNSSEC لنطاقات gTLD - أوه.

هل ذلك إلزامي الآن؟

شخص غير محدد: تلك هي القاعدة العامة. أجل.

جاك لاتور: عموماً، عليهم دعم DNSSEC، لكنهم لا يدعمونه كل الوقت.

شخص غير محدد: هل هناك لائحة منشورة ومحدثة من طرف ICANN؟

جاك لاتور: لا.

شخص غير محدد: سوف أيضاً أتحدث باللغة الفرنسية. سأطرح سؤالاً صعباً بسبب DNSSEC الذي تحدثنا عنه في الجامعة. إنه تكنولوجيا تم نشرها منذ 20 سنة مضت. في الواقع، منذ 19 سنة. لماذا لم يتم نشر DNSSEC في كل مكان اليوم؟ أين هو متوقف؟ لماذا ليس في كل مكان؟ هل هناك مشكل في مكان ما؟

جاك لاتور: إنه متوقف على مستوى أمناء السجلات، خصوصاً الآن. يريد مشغلو DNS توقيع أسماء النطاقات، لكنهم بعيدون جداً عن السجلات لخلق سلسلة DNSSEC. لذلك، أمناء السجلات لا يدعمون DNSSEC، وذلك هو حيث يوجد التوقف. كل الخوادم الكبيرة تدعم DNSSEC افتراضياً. إنه قادم، لكن المشكل الكبير يوجد على مستوى أمناء السجلات.

دان يورك: لدي بضعة كلمات حول ذلك. حسناً، هنا. خصوصاً القبعة الحمراء. تصورت ذلك. وأعتقد أنني سمعت Microsoft هنا أيضاً.

جاك لاتور: ويمكنك وضع هذا على القناة [غير مسموع]

دان يورك: أعرف ذلك. كان يتوجب علي أن يكون لدي ذلك. لدينا الترجمة. تفضل.

شخص غير محدد: أنا [غير مسموع]. أنا محام من باريس، مع نقابة المحامين في باريس. أفترض أنه في هذه المنظمة لأمن DNS، شركة VeriSign التي توفر لنا الكثير من الخدمات، هذه الشركة دعم كبير، التوقيع الإلكتروني الذي يتم استخدامه من طرف الخدمات القانونية في أنحاء العالم ومن طرف الفنيين في مجالي.

هل لديكم علاقات بالأشخاص القانونيين؟ هل لديكم علاقات بهؤلاء الأشخاص؟ في الاتحاد الأوروبي، لديهم تخصيص للبحث في مبادلات الأمن. هناك عقد أوروبي سيكون قيد التطبيق في يوليو وتوصية لاستخدام التوقيع الإلكتروني في أوروبا كلها فيما يخص الأمور القانونية والفنية. وقد قام المعهد الأوروبي للاتصالات بالعمل.

هل لديكم علاقة بالمجال القانوني، بالخبراء القانونيين؟

دان يورك: للأسف باللغة الإنجليزية. لقد طرحت نقطة ممتازة. أنا لست على دراية بذلك التشريع الخاص الحاصل هناك، لكنني أتذكر أشخاص سياسة مجتمع الإنترنت يناقشون هذا. لذا سأحتاج الرجوع إليهم وإيجاد أكثر قليلاً لأنكم بالتأكيد على حق؛ هناك فرصة هناك للنظر في كيف يمكن أن يكون DNSSEC جزءاً من ذلك أو بطريقة ما.

شكرًا على هذا المقترح. هذا ممتاز. سندون ذلك هناك لرؤية ماذا هناك.

لقد كنا نتكلم إلى بعض الأشخاص في قطاع المحتوى - الاستديوهات السينمائية؛ بعض الأشخاص مثل ذلك - حول استخدام DNSSEC لحماية بعض مواقعهم، مجدداً، يتطلعون لضمان وصول الأشخاص إلى هناك. إذن شكرًا لكم على ذلك.

جاك؟

جاك لاتور: سأستمر في الحديث باللغة الإنجليزية. المناقشة حول التوقيعات القانونية، التوقيعات الإلكترونية، مثل [غير مسموع] التوقيعات للنظام القانوني، ووضع رابط لذلك لعالم DNSSEC أو DANE.

في المستقبل، DANE سيكون إطار عمل محتمل للسماح بذلك و DNS العالمي حتى يتمكن الأشخاص والتوقيعات ربما أن يرتبطوا بطريقة ما. لكن ليست لدي فطرة عن كيف أو ما الذي يجب عليكم القيام به. لكن ربما قد يكون تطبيقاً، ينظر في DANE. شكرًا. [غير مسموع]

دان يورك: أية أسئلة أخرى؟ لدينا وقت ربما لسؤال آخر. نعم، هناك؟

شخص غير محدد: مرحباً، أنا أوليفير. وأنا من الكونغو. وأود أن أعرف متى يمكننا معرفة أن اسم النطاق بالفعل مسجل مع DNSSEC؟ لأن لدينا ورشة عمل حول هذا، وقد أدركنا أنه، من أجل معرفة أن النطاق كان اسم، كان عليكم تثبيت برنامج مساعد لرؤية إذا كان ذلك الموقع مسجلاً مع DNSSEC. أود أن أعرف ما الذي يوقف. لماذا لا توجد اليوم أية أدوات لمعرفة إذا كان DNSSEC قد تم تسجياه مثلما نفعل مع شهادات SSL؟

دان يورك: السؤال هو، إذا كان هناك لا [غير مسموع] جواب إذا ما كان اسم النطاق مسجلاً أو لا. هناك برنامج مساعد يمكنك وضعه في ذلك ليظهر لك، لكن لماذا ليس هو جزءاً من ذلك؟

اسمحوا لي بطرح سؤال. كم منكم انتبه للقفل الأخضر على متصفحكم للويب؟ حسنًا. حسنًا. جيد. كم منكم، حينما - نعم، حسناً. كم منكم حين تتلقون ذلك الإنذار أو شيء ما يقول أن الشهادة ليست صحيحة أو شيء مثل ذلك فقط يضغطون عليه؟ حسنًا. أجل.

أحد الأمور التي تم إيجادها هي أن أغلب الأشخاص فقط نوعاً ما يهملون - نعم، نحن نرى القفل، لكن إذا كان هناك مشكل مع القفل، نمر فقط لأننا نريد الوصول إلى الموقع أو شيء مثل ذلك. إذن بعض هذا التحديد المرئي حيث اسم نطاق لديه شهادة TLS أو تم تسجيله تم إظهار أنه لا يعمل حقاً.

ما حصل في فضاء DNSSEC كان هو أنه حصل تحت ذلك المستوى. إذا تم تسجيل اسم نطاق وكان جيداً، سترون ذلك فقط. إذا تم تسجيل اسم نطاق وكان سيئاً، لن تصلوا هناك، أو إذا كان هناك تعارض، أو إذا كان هناك مهاجم يحاول الدخول هناك. تحصل على ما يسمى فشل خدمة في DNS، لنصبح مثل المهتمين بالتكنولوجيا للحظات. لا يمكنك الوصول إلى الموقع. يتم أخذه تحت ذلك. لذا ليس هناك تفاعل مستخدمين بتاتاً. المستخدم لا يراه.

الآن، بصراحة، الطريقة الوحيدة لمعرفة أن نطاقاً تم تسجيله هي استخدام بعض الأدوات الأخرى، بعض المواقع الأخرى التي هي هناك، والتي تسمحك لكم يرؤية ذلك على موقع هناك.

أعتقد أن هناك أشخاصاً سيرغبون في جعل ذلك أسهل لكم لرؤية إذا كان نطاق مسجلاً. هناك متصفح طوره فريق روس قام بذلك. وهناك البرامج المساعدة التي ذكرتها والتي تقوم بذلك.

هناك ذلك النوع من التقسيم. بعض الأشخاص سيرغبون في إظهار ذلك. آخرون سيقولون فقط، "لنجعله فقط آمناً أو غير آمن." إذن الجواب هو، أنا لست متأكداً من متى سنرى ذلك لأنه جزئياً حرب دينية.

روس موندي: حسناً، أيضاً، كما ذكر دان، أظهرت الدراسات أن فعالية وضع مؤشر مرئي لمستخدم هي في الأفضل موضع شك لأنهم عادة يشعرون بأن عليهم الوصول سواء كانوا يذهبون على أي حال وسيميلون للعمل حوله أو إهماله.

أحد الحجج المضادة المرتبطة سواء أو لا مع DNSSEC حاضرة هي أن الكثير من الأشخاص يريدون حقاً أن يصبح ذلك الوضع الافتراضي في كل مكان والذي يحصل والوقت الوحيد حيث ستحتاج مؤشراً هو إذا لم يعمل DNSSEC. إذن الرغبة في الوصول إلى نطقة القدرة على الإظهار، "أوه، هناك مشكل DNS،" وفقط وصفه كمشكل DNS حينما يكون هناك فشل DNSSEC.

هذا أحد أسباب استمرارنا في الحصول على تلك السلاسل التعليمية وورش العمل هو تشجيع الأشخاص. أحب ذلك السؤال. لماذا لا أراه؟ لماذا لا يمكنني الحصول على معلومات أكثر حول هذا؟ ذلك رائع حقاً. تمرير ذلك خارجاً للأشخاص الذين تعمل معهم، إلى موفري الخدمة، إلى إدارة IT خاصتكم.

دان يورك: أنا أعلم أن الوقت قد بدأ يداهمنا. لدينا سؤالان موجزان متبقيان. سأقول أيضاً أننا حين نقوم بذلك، أيضاً، إذا كنتم مهتمين بالمزيد، لدينا ورشة العمل هذه يوم الأربعاء، حيث هناك الكثير من المعلومات.

لنواصل. سؤال؟

نومسا موانيغا: اسمي نومسا. أنا من زيمبابوي. ذكرت شيئاً حول تدفق DNS الإفريقي. انطلاقاً من ملاحظتك، لا يوجد الكثير من DNSSEC الذي يحصل. هل هناك طريقة تحاولون حقاً بناء القدرات خصوصاً لأجل - وكيف؟

دان يورك: الجواب على ذلك هو أن عدد - بمجرد أنتم توقيع جذر DNS في 2010، فقد بدأ الكثير من TLDs الأخرى حول العالم التوقيع على ذلك. يوم الأربعاء صباحاً، سأضع خريطة تظهر النشر. لكن يمكنكم حقاً الوصول إلى هذا. سأخبرك كيف في دقيقة.

الكثير من ccTLDs الإفريقية لم توقع بعد. الآن، هناك أمران يحصلان واللذان يغيران ذلك. قام سيد في الخلف بذكر ورشة العمل التي كانت تحصل. ICANN، مع مجتمع الإنترنت (ISOC)، مع مركز موارد بدء الشبكة (NSRC) كانوا يذهبون، ويعملون في الكثير من الدول، للعمل عادة مع مشغلي شبكة السجل في المجال وغيره لجلب توقيع DNSSEC.

هل هناك أي شخص هنا كان في أحد ورش العمل تلك؟ مارك كان في أحدها. أجل. حسنًا. مارك كان يقوم بها. السيد الجالس هناك قد حضر. حسنًا. ورش العمل كانت تعمل للمساعدة على بناء ذلك.

في أي مكان يمكن أن تجد المزيد هو إذا ذهبت إلى dnssec-africa.org. إنه موقع يتم تسييره من طرف آلان أينا. لا أعلم إذا كنتم تعرفون آلان، لكنه يعمل على ذلك الموقع. هناك مكان هناك يظهر إحصائيات DNS، والذي يظهر أي دول وقعت وأي دول لم توقع، وأيضاً يعطي روابط لإيجاد المزيد حول كيفية الحصول على اتصال أكبر.

أيضاً، في خلف هذا المبيان - وإذا لم تحصل على واحد، فهناك كزيد هنا، ويمكننا تزويدكم بمعلومات أكثر حول هذا - في خلف هذا المبيان، هناك لائحة من الموارد هنا، بما في ذلك المعلومات من برنامج 360 لنشر مجتمع الإنترنت، ومشروع أدوات DNSSEC - عدد من الأجزاء الأخرى من المعلومات هناك. إذن بعض تلك الأماكن حيث يمكنكم البدء كذلك.

هذا أدرك أنه ليس لديه dnssec-africa لأنني تعلمت للتو حول ذلك سابقاً هذا الأسبوع. لم أدرك أن آلان قام بالكثير مع عمله ذلك معه. لكنه عمل جيد هناك.

[هل ذلك] جواب؟ حسنًا. السيد الجالس هناك؟

شخص غير محدد: أهلاً. أنا [غير مسموع] من المغرب. هل يمكننا فقط قول أن أحد أسباب أن DNSSEC بطيء جداً من حيث النشر هو لأن هناك أدوات أخرى تجعل من الأسهل تأمين الحماة من الخطف؟

أيضاً، أن يحصل ذلك على بعض الخطف عن بعد صعب جداً.

دان يورك: الجواب على ذلك هو أنه، في الواقع، نشر DNSSEC كان يتحرك مع - أردناه بالتأكيد دائماً أن يكون أسرع، لكن كما قال وارين، ونحن في حوالي 20% من التحقق، وأعلى في بعض المجالات. لدينا بعض التوقيعات الجيدة الحاصلة في بعض الأماكن.

جزء من القضية هو أن DNSSEC يحل فقط جزءاً من اللغز، صحيح؟ إنه جزء من ذلك. من جانب TLS، هناك عدد من التكنولوجيات الأخرى الموجودة هناك، مثل حصر الشهادة، وبعض الأجزاء الأخرى المستخدمة هناك. لكنهم، مجدداً، يحلون جزءاً آخر من اللغز. إذن DNSSEC يحل لغزه بشكل جيد جداً، ويحل جزءه هناك. لذا كل هذا يتوافق ويتكامل مع بعضه البعض.

شخص غير محدد: كما رأيت، أن DNSSEC يحينا من الخطف المباشر، مثل في محيط آلان وهكذا، لذا هناك طرق كثيرة حيث يمكننا حماية أنفسنا في هذه الأنواع من المحيطات. إذن هذا هو السبب الذي يجعل نشر DNSSEC بطيئاً جداً؟

دان يورك: لست متأكدًا جداً. يمكننا الحديث أكثر قليلاً بعد ذلك، ربما لفهم ذلك قليلاً. هناك بالتأكيد طرق أخرى لمواقع الخطف، وهناك آليات حماية أخرى هناك.

DNSSEC، مجدداً، يحل تلك القضية DNS، ويضمن أن الأشخاص يصلون إلى عناوين IP التي تضعونها هناك. لكن ذلك نوه واحد من الخطف. لكن هناك اختطافات أخرى، أيضاً.

شخص غير محدد: حسنًا. لأنه يجب علينا المرور على هجوم رجل-في-الوسط لتسميم تخزيم مؤقت آخر. لذا يمكننا الحماية من هذا الاستخدام [غير مسموع] أو آليات أخرى.

دان يورك: هل أردت قول شيء؟ لا؟ حسناً، سأقول أن هناك بالتأكيد - DNSSEC هو جزء فقط من دفاع كامل في العمق. نتحدث عن ذلك هنا لأننا في ICANN نتحدث عن DNS. إذن بالنسبة لنا، تأمين DNS هو ما نحن فيه اليوم. من وجهة نظرنا، نحتاج أن يضل بنا DNSSEC إلى إنترنت مفتوح وموثوق يمكننا جميعاً من الحصول على الفرص التي نريد. إذن هذه أداة لدينا للمضي والقيام بذلك.

أوه، وارين يريد قول شيء ما الآن.

وارن كوماري: نعم. أظن أن أمراً جديراً بالذكر هو أن الكثير من الأنواع الأخرى من الهجومات من نوع رجل-في-الوسط تتطلب منك أن تكون محلياً للمستخدم - تسميم DHCP والأمور مثل ذلك، خداع ARP. عليك أن تكون محلياً للمستخدم أو لمسار شبكته.

بشأن التسميم من نوع DNS، إذا لم يكن لديك DNSSEC، يمكنك القيام به من نطاق أماكن أوسع كثيراً. يمكنك القيام به من أي مكان على الإنترنت، ويمكنك أيضاً التأثير علىعدد كبير من المستخدمين. لذلك فإن نطاق الهجوم أوسع بكثير.

تحتاج الكثير من المجموعات المختلفة من الحمايات. يقدم DNSSEC واحدة، لكنه يقدم حماية مفيدة جداً.

دان يورك: أيضاً، الكثير من الآليات الأخرى تسمى الثقة في الاستخدام الأول. يحتاجون أن يكونونا قادرين على ضمان أن يتواصلوا مع المكان الصحيح للبدء. يساعد DNSSEC على توفير تلك الثقة التي تحصلون عليها في المكان الصحيح والوقت الصحيح.

مع ذلك، أود الاختتام لأنني أعلم أننا في نهاية الوقت، إنه هنا. أريد تشجيعكم جميعاً مجدداً: الموارد في الخلف هنا. بالنسبة لأولئك الذين يريدون التعمق أو تعلم المزيد، هناك ورشة عمل DNSSEC يوم الأربعاء. سأذكر أن بدء ذلك قد يكون مهماً لبعضكم لأنه يتحدث عن تطبيقات DNSSEC واستخدامها عبر إفريقيا. هناك لجنة ستضم مارك. وستضم مجموعة من الأشخاص الآخرين. ستضم آلان حيث سيتحدث عن العمل الذي كان يقوم به وآخرين. ذلك الجزء قد يكون محل اهتمام لكثيرين منكم.

وقد تم نشر جدول الأعمال على الموقع الإلكتروني. إنها ورشة عمل DNSSEC ليوم الأربعاء. يمكنكم تصور أية أجزاء من ذلك تودون الحضور لها. نحاول إبقاء ذلك يعمل بشكل صحيح من حيث الوقت حتى تتمكنوا من معرفة في أي وقت يجب عليكم الحضور هناك.

أود منكم الانضمام إلي في جولة تصفيقات لشكر الجميع هنا على هذا. سنكون هنا لبضعة دقائق إضافية إذا كنتم تريدون الحديث معنا. شكرًا.

جاك لاتور: شكرًا.

[نهاية النص المدون]