كوبنهاغن– الاجتماع المشترك: مجلس ICANN ومجموعة الخبراء الفنيين (TEG)
الأربعاء، الموافق 15 مارس 2017 – من الساعة 17:00 إلى 18:30 بتوقيت وسط أوروبا
اجتماع ICANN58 | كوبنهاغن، الدانمارك

ستيف كونتي: إذا كان فيكم من يبحث عن مجموعة القبول الدولي، فقد انتقلت من هذه القاعة إلى B5.1. وهذا لا يعني أننا لا نريدكم هنا، لكن إذا كنتم تبحثون عن شيء ما خلاف جلسة مجموعة الخبراء الفنيين التي تعني بالقبول الدولي، ومقر انعقادها في B5.1. وأنا أرغب في بدء الاجتماع الآن.

ديفيد كونراد: ماذا – أوه، ياللعجب. يمكن أن تبدأ الجلسة. فجون موجود هنا.

>> (بعيدًا عن الميكروفون.)

ديفيد كونراد: بالفعل، لا نزال نقوم بقليل من التغيير الاستراتيجي الآن. ويقول ستيف ولويزويس أنهما في طريقهما، لذا فأنهما سيكونان هنا في غضون لحظات. ونحن نحاول تغيير بعض الشرائح الآن.

>> (بعيدًا عن الميكروفون.)

ديفيد كونراد: حقًا، يمكننا البدء فعليًا ببعض المقدمات، إذا ما حبّذ الأشخاص ذلك. وللسياق، فهي جلسة معنية بتحدي مجلس الإدارة مقابل الخبراء الفنيين. حسنًا. ربما لا.

إنه – لا أعرف، عدد قليل من اجتماعات مجموعة الخبراء الفنيين. وهي معدة للسماح للخبراء الفنيين بتقديم مدخلات لمجلس الإدارة. ونحن لا نقدم مشورة، بل مدخلات. إنها – في الأصل، وهي جلسة مغلقة، غير أننا رفعنا ذلك الغلق برغم ذلك، ونرحب، كما تعلمون، بمشاركة أي شخص مهتم بالأمور البسيطة.

دعونا نبدأ. هل – تعلمون، كان هناك سؤال على ما يبدو عن ما إذا – ما إذا كان، كما تعلمون، اللجنة الاستشارية لنظام خادم الجذر (RSSAC) واللجنة الإستشارية للأمن والإستقرار (SSAC) تمت دعوتهما إلى ذلك أم لا. حسنًا، (أ) فإنها جلسة مفتوحة، (ب) قد يكون هناك بعض الارتباك لأننا – عن ماذا كان ذلك الاجتماع؟ مراكش؟ لقد نسيت أي اجتماع يقصدون، لكننا اضطررنا إلى إلى العودة – اضطررنا إلى إلغاء مجموعة الخبراء الفنيين لتقوم بالأمور المرتبطة بالانتقال، لذلك بدلاً من عقد اجتماع مجموعة الخبراء، قررنا أن يكون لدينا تشكيلة من مجموعة الخبراء/مجلس الإدارة، ولنجعل الأمور مسلية بعض الشيء، وأضفنا أيضًا اللجنة الاستشارية لنظام خادم الجذر واللجنة الاستشارية للأمن والاستقرار، ولذلك كان هناك تشكيلة تضم المجلس/مجموعة الخبراء الفنيين/اللجنة الاستشارية للأمن والاستقرار/اللجنة الاستشارية لنظام خادم الجذر التي أصبحت الآن نوعًا ما شبه تقليدية، ويرحب بأعضاء مجموعة الخبراء وأعضاء مجلس الإدارة في TE– وتجتمع هذه التشكيلة الليلة في روبي عند الساعة 7:00 أو شيء من هذا القبيل.

.7:00 <<

ديفيد كونراد: الساعة 7:00، وتغادر الحافلة عند الساعة 6:45 من امام –

بالفعل، لديك ميكروفون.

>> وبعد انقضاء الجلسة، في الساعة 6:45 تنتظرنا حافلة وافرة السعة عند مركز بيلا، المدخل الغربي، بالقرب من الزاوية من هنا مباشرة.

وعند الساعة 6:45، نرجوكم بالحضور إلى مجلس الإدارة والانضمام إلينا. شكرًا.

ديفيد كونراد: وقد وصل ستيف، كما هو الحال مع جون، ويمكن أن تبدأ الجلسة.

>> (بعيدًا عن الميكروفون.)

ديفيد كونراد: بالضبط. هل ترغب في قول أي شيء الآن؟

ستيف كروكر: بالتأكيد. أعتذر عن التأخير. وأنا سعيد للغاية لرؤيتي العديد من الأشخاص هنا. فهذا أمر رائع حقًا. فديفيد هو المسؤول عن ذلك.

[ضحك]

ديفيد كونراد: حسنًا. دعونا نبدأ بالمقدمات.

مارك، تفضل رجاء. اسمك، نعم، الشركة، اللون المفضل. لا أدري.

مارك بلانكت: مارك بلانكت.

جاي دالي: جاي دالي من نطاق .NZ.

دانيال داردايلر: دانيال داردايلر من W3C.

ليتو إيبارا: ليتو ايبارا من مجلس إدارة ICANN.

كافيه رانجبار: كافيه رنجبر، من مجلس إدارة والقسم الفني.

لارس–جوهان ليمان: لارس–جوهان ليمان، رئيس عمليات خادم ملف الجذر في نت نود.

جورج سادوسكي: جورج سادوسكي، عضو في مجلس إدارة ICANN.

رينالیا عبد الرحيم: رينالیا عبد الرحيم، عضوة في مجلس إدارة ICANN.

باتريك فالتستروم: باتريك فالتسروم رئيس اللجنة الاستشارية للأمن والاستقرار.

أشوين رانجان: أشوين رانجان، موظف في ICANN.

شيرين شلبي:	شيرين شلبي، عضو في مجلس إدارة ICANN.
ماركوس كومر:	ماركوس كومر، من مجلس إدارة ICANN.
تيري ماندیرسون:	تيري ماندیرسون، موظف لدى ICANN، ومدير هندسة نظام اسم النطاق ومدير منطقة في فريق عمل هندسة الإنترنت (IETF) لمنطقة الإنترنت.
ألين دوراند:	ألين دوراند، موظف لدى ICANN، في أبحاث التعداد الإلكتروني للميزات والملاحظات.
آشا هيمراجاني:	آشا هيمرانجاني، من مجلس إدارة ICANN.
باول فيكسي:	باول فيكسي – ضيف مدعو من شركة فارسايت للخدمات الأمنية.
جيريمي راند:	جيريمي راند، مشروع نيم كوين.
بول ووترز:	بول ووترز، منسق علاقات فريق عمل هندسة الإنترنت.

ستيف كروكر:	ستيف كروكر، مجلس إدارة ICANN.
ديفيد كونراد:	ديفيد كونراد، منظمة ICANN.
ستيف كونتي:	ستيف كونتي، موظف في ICANN.
كاثي بيترسين:	كاثي بيترسين، موظف في ICANN.
ويندي بروفيت:	ويندي بروفيت، موظف في ICANN.
جون سوينين:	جون سوينين منسق علاقات فريق عمل هندسة الإنترنت لدى مجلس إدارة ICANN.
دان يورك:	دان يورك، مجتمع الإنترنت مع التركيز على الامتدادات الأمنية لنظام اسم النطاق.
سوزان وولف:	سوزان وولف، مسؤولة التعامل مع مثيري المشاكل العشوائيين في اللجنة الاستشارية للأمن والاستقرار، واللجنة الاستشارية لنظام خادم الجذر.

وارن كوماري: وارن كوماري، منسق علاقات فريق عمل هندسة الإنترنت.

إد لويس: إد لويس، موظف لدى ICANN، في أبحاث التعداد الإلكتروني للميزات والملاحظات.

روي آريندس: روي آريندس، موظف لدى ICANN، في أبحاث التعداد الإلكتروني للميزات والملاحظات.

مات لارسون: مات لارسون، موظف لدى ICANN، في أبحاث التعداد الإلكتروني للميزات والملاحظات.

فرانسيسكو دا سيلفا: فرانسيسكو دا سيلفا من المعهد الأوروبي لمعايير الاتصالات والشركة التي أعمل بها عالمية النطاق، مقرها السويد.

هوارد بن: هوارد بن، أمثل المعهد الأوروبي لمعايير الاتصالات أيضًا.

جولي هامر: جولي هامر، من اللجنة الاستشارية للأمن والاستقرار.

رود راسموسن: رود راسموسين، اللجنة الاستشارية للأمن والاستقرار.

>> (ذاكرًا الاسم) من قطاع معايير الاتصالات في الاتحاد الدولي للاتصالات.

أدييل أكبلوغان: آدييل أكبلوغان من موظفي ICANN من قسم المشاركة الفنية.

غريغ آرون: غريغ آرون، من اللجنة الاستشارية للأمن والاستقرار.

مارتن بوترمان: مارتن بوترمان، من مجلس إدارة ICANN.

جاب أكيرهوس: جاب أكيرهوس، من المؤتمر التحضيري للجنة الاستشارية للأمن والاستقرار واللجنة الاستشارية لنظام خادم الجذر.

لويزويس فان دير لان: اعتذر عن التأخير. لوسويس فان دير لان، من مجلس إدارة ICANN.

جون كرين: كنت هناك متواريًا في الخلف وبرغم ذلك يجب أن أذهب إلى الأمام. جون كرين، جون كرين، مسئول المرونة والاستقرار والشفافية الأول في ICANN.

ديفيد كونراد: حسنًا. شكرًا جزيلاً.

الأجندة الأولي موجودة على الشاشة. إنها تكون جلسة ترحيب وأعمال إدارية.

وذلك فقط لتكرار ما ذكرناه سابقًا، وإذا ما كنتم تبحثون عن اجتماع الفريق التوجيهي للقبول الدولي، فقد تم نقله إلى B5.1، التي تقع أسف الرواق مباشرة. برغم ذلك، فإننا نرحب بكم هنا أيضًا. وهي جلسة معنية بتحدي مجلس الإدارة مقابل الخبراء الفنيين.

ولنبدأ في الموضوع، إنني أعتقد أننا سوف نبدأ بعرض تقديمي يقوم به جيريمي راند من مشروع نيم كوين يتحدث فيه عن النيم كوين. لذا، يمكنك البدء جيريمي إذا ما كنت ترغب في ذلك.

جيريمي راند: مرحبًا. أدعى جيريمي راند من نيم كوين، اسمحوا لي أن أبدأ العرض.

بإيضاح تام أولاً. إنني أحد مطوري النيم كوين الأكثر نشاطًا ولست على دراية بأي مطورين للنيم كوين لا يتفقون مع ما أقوله في هذا الحديث. برغم ذلك، لا يمكنني التحدث إلى جميع المطورين عن كل شيء. فمشروعنا مفتوح المصدر وهو ليس لديه هيكل تنظيمي واضح، عليكم فقط أن تكونوا على علم بذلك.

وقد تم إعداد هذه المحادثة بالتعاون مع هوغو لاندو.

وبالتالي فإن الحافز الأساسي لمشروع نيم كوين هو أن يتصرف البشر بصورة غير حتمية، وبالتالي، فأي نظام يشغله البشر سوف يتصرف بصورة غير حتمية.

وعلى وجه الخصوص، حتى وإن كان النظام لديه قواعد أساسية من المفترض أنها لا تنتهك، فإن القواعد الأساسية التي ينفذها البشر سيتم إنفاذها بشكل متضارب.

وهناك مثال على ذلك، وضع الدستور الأمريكي قواعد أساسية تقول بحظر التعذيب والمراقبة بالجملة. ولسوء الحظ، ينفذ هذه القواعد الأساسية البشر، وبالتالي، كما تعلمون جميعًا، لا تنفذ هذه القواعد في أي مكان قريب بالصورة الحتمية التي نأملها.

وسيكون تصرف البشر في المستقبل البعيد غير حتمي بصورة كبيرة.

وعلى سبيل المثال، توقع نتائج الانتخابات تصبح أكثر صعوبة في المستقبل، وبالتالي، فإن توقع المناخ السياسي في دولة ما يكون أكثر صعوبة تبعًا لذلك كلما تعاقبت الأزمنة.

ويتم تشغيل نظام اسم النطاق، إلى حد كبير، علي يد البشر. ويشكل ذلك خطرًا لأن الأشخاص المدرجين في تشغيل نظام اسم النطاق يمكن أن يتصرفوا بصورة غير حتمية.

وقد يرتكب أمين السجل الخاص بكم خطأ ويسمح لشخص آخر بتغيير سجلاتكم، أو قد يتم إسقاط الحكومة التي لديها نطاق المستوى الأعلى لرمز البلد بعد 10 سنوات من الآن وتقرر الحكومة الجديدة أنها لا ترغب في اسمكم ومن ثم تستحوذ عليه، أو قد يؤدي الضغط السياسي في المستقبل إلى تنفيذ ICANN سياسة جديدة التي لم تتفقوا عليها الآن.

وقد يحدث أي مما سبق وهو أمر يدعو للقلق.

وهنا يأتي دور النيم كوين التي تعتبر تجربة للتبين يكون بمقدورها بناء شيء ما يماثل على نحو غامض نظام اسم النطاق ولكن مع قدر بسيط من المشاركة البشرية قدر الإمكان، وبالتالي إنشاء نظام يماثل نظام اسم النطاق الذي يتصرف بشكل أكثر حتمية مما يفعله نظام اسم النطاق. ونأمل أن يتسم نظام كهذا بمزيد من الموثوقية والأمان مقابل أشكال الإخفاق التي يتسبب فيها البشر نظرًا لحتمية الجهاز بصورة كبيرة.

واسمحوا لي أن ألقي نظرة عل بعض أنظمة المعرفات الحالية حيث يمكن أن نرى كيفية مقارنتها بالنيم كوين.

التسمية اليدوية علي أي موقع، وهي أشياء كملفات المضيف، لا تمتلك مساحة اسم عالمية، بمعنى أن الأسماء تكون ذات معنى فقط على الصعيد المحلي، غير أنها آمنة من الأطراف البشرية الأخرى غير الحتمية ولديها أسماء ذات معنى بشري، بالتالي فهذا أمر جيد.

أما التسمية التدريجية مثل نظام اسم النطاق لديها مساحة اسم عالمية لكنها غير آمنة من الأطراف البشرية الأخرى غير الحتمية. ولديها أسماء ذات معنى بشري. ولديها قابلية استعمال جيدة غير أنها محفوفة بالمخاطر كجذر الثقة.

ولدى معالجة المحتوى مثل بت تورنت، حيث يكون الاسم هو التجزئة، مساحة اسم عالمية وتكون آمنة من الأطراف البشرية الأخرى غير الحتمية ولديها أسماء ذات معنى بشري ولا يمكن تغيير المحتوى.

وبديل ذلك هو الاسم الذي يكون مفتاحًا عامًا. وأشياء مثل نطاقات ONION. التي تستخدمها شبكة "تور". وهذه الأشياء لديها مساحة اسم عالمية وتكون آمنة من الأطراف البشرية الأخرى غير الحتمية ولكنها ليست لديها أسماء بشرية ذات معنى. وبالرغم من ذلك، يمكن تغيير المحتوى. وهذا النوع من الأنظمة يكون آمنًا كجذر الثقة لكنه يعاني من قصور في قابلية الاستعمال بصورة كبيرة. وسوف يرى المستخدم محدد موقع المعلومات كما ترونه على الشاشة عندما يحاول كتابة شيء ما فيه.

وفي الحقيقة، إنني أكذب. فشبكة "تور" تقوم بعمل ترقية أمان فورًا وعند الانتهاء، سوف تبدو الأسماء مثل ذلك بالفعل.

[ضحك]

جيريمي راند: أجل. لعلكم لاحظتم أنه في الشرائح السابقة كان يوجد ضابطان وعلامة X واحدة وهذا هو مثلث زوكو. وخمّن زوكو ويلكوكس أنه من المستحيل تحقيق هذه الثلاثة مرة واحدة.

وبالانتقال إلى موضوع مختلف نوعًا ما، تشهد السجلات العامة للإلحاق فقط ازدياد شعبيتها لضمان المساءلة. والمثال الأكثر نجاحًا لذلك يتجلى في شفافية شهادة Google. فكل شهادة منفردة مستخدمة في الويب العام توضع في السجل للإلحاق فقط، ومن المحتمل أن تطلب المستعرضات في نهاية الأمر الشهادات ليتم تسجيل الدخول لتكون صالحة.

وحتى وإن كنتم ترغبون في مواصلة التحكم في نظام ما، فقد ترغبون في نشر جميع الإجراءات.

شفافية الشهادة هي سجل للإلحاق فقط للشهادات غير أنها مناسبة جدًا للاستخدام مع الأنظمة مثل نظام اسم النطاق، والسبب وراء ذلك هو من يستطيع الكتابة للسجل؟ أي شخص. ولكن الشهادات الواردة من الجهات المانحة للشهادات هي فقط التي يمكن كتابتها. وذلك أمر جيد لضمان عدم ذهاب السجلات مع البيانات العشوائية إلى بريد غير مرغوب فيه، غير أن قائمة يدوية بالجهات الموثوقة تكون نوعًا ما معرقلة.

يعد النيم كوين سجلًا للإلحاق فقط لتسجيلات الأسماء وتحديثاتها. بالرغم من ذلك، بخلاف شفافية الشهادة، يتم تنفيذ النيم كوين باستخدام سلسلة الكتل، بالتالي يمكنها منع البريد غير المرغوب فيه بفرض تكلفة اقتصادية لكتابة البيانات، وتكون هذه التكلفة صغيرة لكنها فعالة جدًا، ويثني ذلك العوامل السيئة عن الاستحواذ الكلي على الأسماء دون الاعتماد على قائمة يدوية بالكيانات الموثوقة.

وتمتلك النيم كوين مساحة اسم عالمية، وتكون آمنة من الأطراف البشرية الأخرى غير الحتمية ولديها أسماء ذات معنى بشري، لذا فهي تعد حلاً لمثلث زوكو. وتعني النيم كوين أن السجل المعني بالإلحاق فقط الخاص بالتسمية يمكن تشغيله كمنتدى مفتوح، حيث يعمل على تعزيز كيانها. ويمكن إجراء المساءلة والشفافية بطريقة سرية للصالح العام القابل للتحقق. وبالنسبة لاستقلالية نظام القواعد التي تستخدمه النيم كوين للأسماء، فطبيعتها كسجل للإلحاق فقط تعني أنه إذا قام عنصر سيء بعمل شيء ما، فأنت تعرف دائمًا ذلك.

وكتجربة فكرية، فضعوا في اعتباركم فكرة منطقة الجذر المسؤولة. فيمكن أن ترضي المساءلة الأطراف المتشككة بخلاف ذلك حيث لا يستمر أي شيء غير مخطط له.

كمثال افتراضي، فإن الحفاظ على منطقة الجذر كسجل للإلحاق فقط يرضي الدول في كل أنحاء العالم حيث لا يساء استخدام تحكم الولايات المتحدة حتى في المستوى المشترك بين الحكومات.

ويمكن لخوادم الجذر أن تتغذى مباشرة من السجل. ويمكن أن ترضي منطقة الجذر المحافظ عليها كسجل للإلحاق فقط الدول التي، على سبيل المثال، لن يتدخل نطاق المستوى الأعلى لرمز البلد الخاص بهم في أسباب سياسية، وتستخدم نظائر المراقبة الجذرية نوعًا ما من قبل الدول للتحقق من بعضهما بعضًا بموجب سلم ضمان معاهدة حظر التجارب النووية. فالثقة لا تغني عن التحقق. وللإيضاح، إنني لا أوصي بتنفيذ هذه الفكرة الخاصة في نظام اسم النطاق لكن أوصي بإجراء دراسة حالة افتراضية هامة.

وللمضي شيئًا فشيئًا، فالمشكلة ذات الصلة هي البنية التحتية العامة PKI. أما نظام هيئة منح الشهادات المستخدم اليوم فهو نظام صعب حتى مع شفافية الشهادة. والمشكلة الأساسية هنا تتجلى في أنه يوجد العديد من البشر غير الحتميين المدرجين ممن يمكنهم ارتكاب أخطاء. وقد تحسن الامتدادات الأمنية لنظام اسم النطاق التحقق المستند على DNS للوحدات المسماة DANE، التي تخزن بيانات أمان طبقة النقل TLS، بدلاً من تحقق هيئات منح الشهادات منهم، من الوضع. ولسوء الحظ، يوجد هناك مسائل سياسية أيضًا. وينتاب بعض الناس القلق بشأن إمكانية إساءة الاستخدام من جذر نظام اسم النطاق أو مشغلي نطاق المستوى الأعلى.

ومرة أخرى تكمن المشكلة هنا في أن جذر نظام اسم النطاق ومشغلي نطاق المستوى الأعلى يتضمنوا بشرًا أيضًا. لذا، لا يعتبر ذلك حلاً نهائيًا لمشكلة تضمين البشر. وقد تقدم النيم كوين مزايا الامتدادات الأمنية لنظام اسم النطاق والتحقق المستند على DNS للوحدات المسماة DANE لهذا الغرض دون مشاكل سياسية.

وبالتالي، فإننا لا نتوقع أن معظم البرامج أو حتى معظم مكتبات قرارات الأسماء ستكون على علم بالنيم كوين مباشرة. وبدلاً من ذلك، فإننا نتوقع أن يتم تثبيت برنامج جسر النيم كوين إلى نظام اسم النطاق محليًا، بنقل استفسارات نظام اسم النطاق إلى استفسارات النيم كوين وتحويل ردود النيم كوين إلى نظام اسم النطاق.

يستخدم النيم كوين نطاق المستوى الأعلى BIT.، ولا يتم تسجيله فوريًا مع ICANN أو فريق عمل هندسة الإنترنت مباشرة. ونود أن نجد طريقة عملية لتثبيت ذلك. وإننا ندرك أنها مشكلة فعلاً. فعلى سبيل المثال، قد نستخدم تسجيلات الاسم خاص الاستخدام، مثل نطاق ONION. من قبل شبكة "تور".

ويعمل مرجع التحديد الخاص بنا الذي يدعى نظام اسم النطاق للنيم كوين (NCDNS) كخادم نظام اسم النطاق الرسمي لنطاق المستوى الأعلى BIT. الذي يعمل على مضيف محلي. وينشئ مستخدمو الامتدادات الأمنية لنظام اسم النطاق وقت تثبيت، ونحاول عن قصد أن نحافظ على تحديد اسم نطاق النيم كوين متمتعًا بسهولة التخطيط لنظام اسم النطاق ليتسنى استخدام برنامج الجسر بكل سهولة.

وإذا رغبتم بشكل افتراضي في استخدام ذلك، يمكنكم إبلاغ خادم نظام اسم النطاق المتكرر، على سبيل المثال، خادم "Unbound " لاستخدام الامتدادات الأمنية لنظام اسم النطاق باعتباره موثوق به لنطاق BIT. ودعمه بالمفتاح العام للامتدادات الأمنية لنظام اسم النطاق الخاص بنظام اسم نطاق النيم كوين. ونظريًا، يجب أن يعمل كل شيء مباشرة. وما ذلك إلا خطوط قليلة في unbound.com.

ومن الناحية العملية، يوجد بعض ميزات نظام اسم النطاق التي لم يجري دعمها بشكل موسع. فعلى سبيل المثال، التحقق المستند على DNS للوحدات المسماة DANE لأمان طبقة التنقل TLS. وبالتالي، علينا أن نقوم ببعض التخصيصات المضاعفة غير الاعتيادية لنجعل ذلك يجدي نفعًا. وإنني كنت بالفعل أحاول ذات مرة أن أتتبع عدد الطبقات المختلفة للتأثير الكبير الذي لا يقاوم التي نستخدمها للقيام بعمل التحقق المستند على DNS للوحدات المسماة DANE بشكل مناسب للمستعرضات التي لا تدعم التحقق المستند على DNS للوحدات المسماة DANE لأمان طبقة التنقل TLS. وتوقفت عن العد عند خمس طبقات من التأثير الذي لا يقاوم.

لذا، ما هي بعض حالات استخدام العالم الواقعي حيث يمكن أن يساعدنا التصرف الحتمي للنيم كوين؟ حسنًا، دعونا نقول أنكم تحاولون شراء أو بيع اسم ما. ففي نظام اسم النطاق، شراء أو بيع اسم يتضمن عادة خطر الطرف النظير، وقد تضطرون إلى الاعتماد على وكيل إيداعات للحد من خطر الطرف النظير.

وفي النيم كوين، يمكن للبائع والمشتري إنشاء معاملة معًا بحيث يتم الدفع للبائع وينقل الاسم إلى المشتري. وذلك يقضي على خطر الطرف النظير دون الحاجة إلى خدمات وكيل الإيداعات.

وهو أمر رائع، ولكن ماذا لو لم يرغب البائع والمشتري في التحدث لبعضهم بعضًا لإنشاء معاملة ذرية؟ ويمكنكم شراء أو بيع العروض. ثم إن طريقة سير العمل تنشئ أشياء مثل ذلك. ويمكن لأليس أن تنشئ عرض بيع. وإنني أرغب في بيع اسم النطاق "example.bit" من أجل 100 نيم كوين. وتوقع أليس على عرض البيع بمفتاحها الخاص الذي يثبت أنها تملك "example.bit" وأرغب في نقله مقابل 100 نيم كوين. ويمكن لأليس نشر عرض البيع الموقع على المنتدى أو باستبين أو أيّ من هذا القبيل.

يشاهد بوب العرض ويرغب في شراء "example.bit". ويمكن لبوب إتمام العرض بالتوقيع عليه بمفتاحه الخاص الذي يضم 100 نيم كوين. وهذا العرض يكون معاملة نيم كوين صالحة في الوقت الحالي. ويمكن لبوب إذاعة شبكة النيم كوين دون الاتصال بأليس مرة أخرى.

فقد حصلت أليس على المدفوعات. واستلم بوب النطاق. وتكون هذه المعاملة ذرية. وليس هناك خطر من طرف مناظر ولا تستدعي الحاجة إلى وجود وكيل إيداعات. ويناسب ذلك عروض الشراء وعروض البيع. ويدعم بروتوكول النيم كوين حالة الاستخدام هذه بالفعل، كما ستأتي الأدوات المناسبة للمستخدم قريبًا آملين ذلك.

بالإضافة غلى ذلك، هناك مثال آخر لحالة الاستخدام وهو أن الاسم يكون مملوكًا عادة بمفتاح خاص منفرد لكن يمكنكم أيضًا امتلاكه بمفاتيح خاصة متعددة حيث ينبغي أن تكون

مفاتيح الوزن الثابت موجودة لعمل تحديث. ويمكن أن يشكل ذلك حماية مفيدة ضد مفتاح منقوص منفرد. فعلى سبيل المثال، يمكن أن يكون لدى كل عضو في مجلس الإدارة مفتاح خاص وقد يتطلب تحديث الاسم أغلبية مطلقة من المجلس. ومرة أخرى يدعم بروتوكول النيم كوين حالة الاستخدام هذه، كما ستأتي الأدوات المناسبة للمستخدم قريبًا آملين ذلك.

ويمكن أن يسمح النيم كوين أيضًا ببناء سياسات تحديث مرنة جدًا، التي يمكن استخدامها لتخصيص الأشياء استنادًا إلى احتياجات الأمان وتصميم تجربة المستخدم "UX" لمالك الاسم. فعلى سبيل المثال، دعونا نقول أن أليس لديها اسم لكنها ترغب في الحد من خطر سرقة مفتاحها الخاص دون التسبب في خطر الطرف المناظر بصورة كبيرة. بالتالي، يمكنها إنشاء سياسة لشيء من هذا القبيل: يمكن لأليس أن تتعاقد مع ترنت لتشغيل خدمة مصادقة ثنائية. ويمكن لها بعد ذلك تحديث اسمها باستخدام بيانات تقديرية، إذا ما وقعت تورنت على تحديثاتها. وتعد تورنت فقط بأن تقوم بذلك بعد التحقق عبر المصادقة الثنائية.

ولكن بالإضافة إلى ذلك، يمكن لترنت التوقيع المسبق على معاملات خاصة لأحداث معينة حيث قد ترغب أليس في القيام بشيء ما دون الحصول على موافقة تورنت في وقت لاحق. فعلى سبيل المثال، قد ترغب أليس في أن تلغي سجل TLSA الخاص بها بالتالي إذا كان خادم الويب الخاص بها تعرض لخطر، فيمكنها أن تلغي الشهادة بسهولة. أو قد ينتابها شعور بالقلق بأن تورنت قد يختفي أو يتنصل من الأعمال أو يفقد مفتاحه الخاص. بالتالي، يمكن تحديد هذه السياسات استنادًا إلى القيود القابلة للتعديل. ولا يمكن أن ينقل تورنت أو يحدّث تاريخ اسم أليس دون الحصول على توقيع أليس، ويمكن لأليس أن تتحقق من موثوقية المعاملات الموقعة مسبقًا وأنها محمية من تورنت قبل أن تطبق هذه السياسة على اسمها. وتحدد هذه السياسات بلغة برمجة ويتم تنفيذها بنفس المستوى الذي يكون عليه التوقيعات القياسية.

ولا تعني النيم كوين إزاحة أمنار السجل. ففي النيم كوين، قد يبدو "أمناء السجل" إلى حد كبير كتورنت. ولكن النيم كوين لا تعني أن أمناء السجل لديهم قدرة أضيق بكثير لإيذاء

عملائهم من نظام اسم النطاق، سواء كان هذا الإيذاء عرضيًا أو كيديًا. وقد ينتهي ذلك إلى أن يخفض أمناء السجل موازنات الأمان الضرورية.

وهناك خدمات مثل تورنت غير متاحة للنيم كوين إلى الآن ، غير أنني أود أن أرى خدمة مثل هذه. وكحالة استخدام أخرى، استهدفت البنية الأساسية لنظام اسم النطاق بهجمات الحرمان المنتشر للخدمة الاخيرة، على سبيل المثال، الهجوم ضد بريان كريبس. وقد اقترح بعض الناس أن النيم كوين قد يكون دفاعًا فعالاً. والآن، من غير الواضح لي كيف للنيم كوين أن تقف في مجابهة تهديد الحرمان المنتشر للخدمة.

وبالرغم من ذلك، خضعت شبكة البت كوين لاختبارات إجهاد، التي تمثلت بصفة أساسية في محاولات هجوم حجب الخدمة في السنوات القليلة الماضية. وقد تم إجراء اختبارات الإجهاد على يد شركات تستهدف الربح التي امتلكت حوافز مالية لتحاول أن تجعل شبكة البت كوين تبدو ضعيفة ضد هذه الخدمات. وكانت شبكة البت كوين غير متأثرة إلى حد كبير. هل ستكمل النيم كوين بشكل جيد؟ أم هل سيكون لدى المهاجمون مواردًا مماثلة مثل مختبرو إجهاد البت كوين؟ هذا أمرٌ يصعب البت فيه. لكني أعتقد أنها حالة استخدام مثيرة للاهتمام. وأود أن أرى مزيدًا من البحث فيما يتعلق بذلك في المستقبل.

ولامتلاك هذه الحتمية، برغم ذلك، علينا أن نعد بعض المبادلات. وهناك أحد الأمثلة على ذلك، وهي أن معاملات النيم كوين غير قابلة للإلغاء. وكنتيجة لذلك، إذا تم نقل الاسم إلى مالك جديد، لا يمكن للمالك القديم أن يستعيده دون توقيع المالك الجديد. وهذا يعني أن أسماء النيم كوين تكون ضعيفة نوعًا ما للاستحواذ العدائي للبرامج الضارة. وبهذا الشأن، قد يكون الخطأ البشري من مالك الاسم مشكلة أيضًا.

وبعض الحلول المطروحة لذلك سوف تتضمن الحفاظ على مفاتيحك الخاصة في آلة ذات فجوة هوائية أو من المحتمل تخصيص توقيعات متعددة أو سياسات مصادقة ثنائية للأسماء، كما ذكرت آنفًا. ولن يكون كل ذلك سيئًا حقيقة. وقد سمعت خبراء الأمن يعلقون بأن واحدة من أفضل المزايا العامة للبت كوين التي لاقت رواجًا هي أن الناس قد أخذوا أخيرًا أمان

نقطة النهاية بجدية. ونظرًا لأن البت كوين أصبحت أكثر نضجًا، فأعتقد أنه من المحتمل أن يتحسن أمان نقطة النهاية فعليًا. وبالتالي، قد يسبب ذلك مشاكل أقل في المستقبل.

وتتجلى المبادلة الاخرى في أن النيم كوين ليس لديه قصد بشري غير حتمي حيث تكون تسجيلات الاسم صالحة. ولهذا السبب فهو يمتلك مزايا أمان وكثير من المقاومة للمسائل السياسية. وبالرغم من ذلك، يعني ذلك أيضًا أنه إذا سجل شخص ما اسم ينتهك علامة تجارية ما، فليس هناك طريقة سهلة لتعطيل تسجيل الاسم. وقد تضطرون إلى التفاوض مع الشخص الذي قام بالتسجيل.

وهذا الأمر ملازمًا بصورة كبيرة لتعريف انتهاك العلامة التجارية. وتحديد ما إذا كان الانتهاك الذي حدث يتطلب بشرًا، وأن النيم كوين صمم صراحة لكي لا يشغله البشر.

أما الحل المؤقت لذلك فهو أن يختار المستخدمون قائمة أسماء انتهاك علامات تجارية معروفة التي تم حظرها في مكان ما بين عميل النيم كوين ومستعرض ويب المستخدم. فعلى سبيل المثال، فإن برنامج نظام اسم النطاق المستخدم ليكون جسرًا لتطبيقات النيم كوين إلى نظام اسم النطاق قد يدعم ذلك كخيار. ويوجد بالفعل بنية أساسية حالية لأشياء من هذا القبيل. وتعتبر فيس تانك مثالًا على ذلك.

أما التنبيه الأول فهو أن أي مستخدم يرغب في عرض اسم ينتهك علامة تجارية يمكن أن يعيق الحظر عن عمد. ولكن نظرًا لأن غرض قانون العلامات التجارية هو تجنب التسبب في الارتباك للمستهلك، فمن المحتمل ألا تكون هذه مشكلة كبيرة جدًا. ومن المتوقع أن المستخدم الذي يؤدي ذلك يعرف بالفعل ما يقومون به. وأما التنبيه الآخر فهو أن أحد الأشخاص يمكنهم شراء اسم انتهاك بمفردهم لغرض بيعه إلى مالك العلامة التجارية الشرعي. وبسبب كلفة أسماء التسجيل، من الصعب لأي فرد أن يستحوذ على عدد كبير من الأسماء بهذه الطريقة، كما هو الحال في كيفية تخفيض كلفة أسماء نظام اسم النطاق للاستحواذ.

وتعد المبادلة الأخرى ذات خصوصية. ونظرًا لعمومية المجموعة الكاملة لمعاملات النيم كوين، يمكن لأي شخص إجالة النظر في المعاملات. أما تحليل الرسم البياني للمعاملات

فيجعله سهلاً للغاية للاستدلال إذا جرى إتمام معاملتين على يد شخص واحد. ويؤثر ذلك أيضًا على البت كوين. وبالتالي، يعني ذلك، إذا قمتم بتسجيل اسمين من أسماء النيم كوين لغرضين مختلفين، فمن المحتمل أن يكون سجل عام الذي جرى تسجيل الاسمين فيه على يد نفس الشخص.

وإذا اشتريتم النيم كوين الخاص بك من شخص آخر، فمن المحتمل أن يروا ما هي الأسماء التي سجلتها معهم. أما الحل المؤقت لذلك فهو شراء النيم كوين بطريقة دفع لا تخلف ورائها سجل عام. بمعنى أنه يتعين عليك ألا تستخدم البت كوين لشراء النيم كوين إذا ما قيمت خصوصيك. وعليك أيضًا أن تستخدم أزواج مفاتيح عمومية وخاصة منفصلة لكل اسم تشتريه بحيث لا يكونوا قابلين للربط في الرسم البياني للمعاملة. وقد تكون المعاملات البنكية طريقة جيدة لشراء النيم كوين دون أن تخلف ورائها سجل عام. وبالإضافة إلى ذلك، كان هناك مساعي تجريبية تبذل لجعل العملات مماثلة بالبت كوين التي لديها خصوصية جيدة مثل عملة Monero وZcash التي يمكنك استخدامهما لشراء النيم كوين ومن ثم الحصول على الأسماء. ولهذه العملات عوائقهم الخاصة، ولكن قد يكونوا نافعين لبعض المستخدمين.

وبوجه عام، يحتوي التنفيذ المرجعي للنيم كوين على خصوصية ضعيفة للغاية ويجعل من الصعب منع العامة من معرفة أن كل الأسماء الخاصة بك لديها ملكية مشتركة. وإننا نرغب في إضفاء تحسينات على ذلك نظرًا لأهميتها.

أما الخيار الأخير فهو أمان طبيعة النيم كوين ذات الارتباط فقط. وتكون كل خصائص الأمان التي يضمها النيم كوين قابلة للتحقق عن طريق التشفير مع استثناء واحد رئيسي، وأن حماية ترتيب عمليات اسم النيم كوين لا تكون آمنة عن طريق التشفير. وبدلاً من ذلك، فالأمر فقط معني بالأمان الاقتصادي، بمعنى إنه سيكلف الكثير من المال لإعادة ترتيب عمليات الاسم. وكلما كان عليك العودة بالتاريخ أكثر، فالكثير من المال سيتم إنفاقه. ويفترض النيم كوين عادة أن الترتيب من المحتمل أن يكون ثابتًا لما يصل إلى

نحو ساعتين بعد إجراء عملية الاسم. غير أن ذلك لا يكون مضمونًا عن طريق التشفير. ويكون ذلك مرجحًا واقتصاديًا بشكل لا يثير أي لبس، لذلك فهو أضعف بكثير.

لذا، كيف يكون ذلك مفيدًا للهجوم العملي؟ حسنًا، إذا كنت قد أعدت ترتيب المعاملات العائدة عند تسجيل الاسم، يمكنك وضع عملية تسجيل لهذا الاسم قبل التسجيل الشرعي، وبالتالي سرقة الاسم.

ويمكنك أيضًا أن تعيد ترتيب عمليات التجديد الخاصة بالاسم للإجراء بعد فترة انتهاء الصلاحية، التي تلزم الاسم بالانتهاء وتسمح لك بتسجيله بنفسك. ولم يحدث أي من ذلك في الواقع الفعلي للنيم كوين. ولكن إذا لاقى النيم كوين استخدامًا متزايدًا، فالعديد من الناس قد يحاولون القيام بذلك.

وتعاني البت كوين من نفس المشكلة هنا. ولكن نظرًا لأن اقتصاد البت كوين يتميز بأنه يفوق النيم كوين، فإن البت كوين يحصل على مزيد من الأمان ضد الهجوم. وهناك الكثير من الأبحاث الفعالة لحل مشكلة سلاسل الكتل الثانوية التي تكون أقل أمانًا من البت كوين. ويعتبر هذا الأمر جزئيًا لأن هناك الكثير من التحسينات أدخلت على البت كوين، بما في ذلك بعض مما تم دفعه من قبل الشركات الممولة تمويلاً جيدًا، تكون أسهل بكثير بالنسبة للنشر إذا ما تم حل هذه المشكلة. وبالتالي، فإننا نتابع مجال الأبحاث عن كثب. ونأمل بإحراز تقدم في القريب العاجل.

ولا يوجد بين تلك الحلول المؤقتة التي ذكرتها للتو للبرامج الضارة والعلامات التجارية والخصوصية شيء دقيق تمامًا كتلك الإجراءات المضادة المتخذة مع نظام اسم النطاق. والعثور على المزيد من الإصلاحات الرائعة يعتبر مشكلة بحثية مفتوحة. ولهذا، ولأجل العديد من حالات الاستخدام في الحياة العملية، من المحتمل أن تكون هذه الحلول المؤقتة كافية.

حسنًا. إذًا، أين يذهب هذا المشروع؟ حسنًا، لسوء الحظ، من الصعب تثبيت النيم كوين حاليًا، لا سيما إذا ما كنتم ترغبون في دعم أمان طبقة النقل TLS للعمل. ويُعزى هذا الأمر أساسًا إلى أنه غير مشغل تشغيلًا أوتوماتيكيًا في عملية التثبيت. ولقد تلقينا التمويل

للتو من منظمة شبكة إنترنت نيوزيلندا NLNet وصندوق زيادة حماية الإنترنت بموازنة من وزارة الشؤون الاقتصادية بنيوزيلندا. وسوف يستخدم هذا التمويل لتحسين قابلية الاستعمال ودعم التطبيق لاستخدام النيم كوين كبنية تحتية عامة لأمان طبقة النقل. وأما الهدف النهائي هنا فيتمثل في أن دمج النيم كوين مع نظام تحليل الاسم الخاص بالكمبيوتر ومع تطبيقات أمان طبقة النقل TLS الخاصة بمستعرضات الويب سيكون قابلًا للتثبيت بخطوة واحدة. لذا، على سبيل المثال، إذا كنت على نظام Windows، فإنك ستشغل ".exe installer". وإذا كنت على نظام "Debian"، فإنك ستشغل ".deb package".

وسوف يستخدم هذا التمويل أيضًا لتحسينات تصميم تجربة المستخدم ومالكي الاسم وتحسينات إمكانية التوسع والأداء. وسأقوم أنا ومعي هوغو لاندو وبراندون روبرتس وجوزيف بيش بإنجاز هذا العمل بشكل أساسي.

ونحن نشارك أيضًا بفعالية في مشروع "تور". وتضم قاعدة مستخدمي تور متطلبات أمان خاصة التي لا تكون مناسبة تمامًا لنظام اسم النطاق. وهم يستخدمون نطاق ONION. الآن، الذي لا يكون ذي معنى بشري، وسيزداد الأمر سوءًا عندما يتم نشر ترقية الإصدار الثالث لخدمات "Onion" كما أوضحت سلفًا. وتكمن المشكلة في أن البشر من الناحية النفسية لم يتحققوا عادة من عنوان "onion" المطوي الذي يعني أن المحتالين ينشئون على الفور بصورة عشوائية صورًا مسبقة جزئية لعناوين ".ONION" الحالية لانتحال شخصيتها. وتعتبر شبكة تور مرشحًا جيدًا للاستخدام المبكر للنيم كوين. ومن المحتمل أن يتعايشون مع الحالة القائمة لخيارات النيم كوين، ومع الاستثناء المحتمل لمشكلات الخصوصية، لأن جميع الخيارات الأخرى المتاحة لا تلبي احتياجات أمان تور. وأعتبر من يقود حملة التوعية بمشروع تور في الوقت الحالي.

وبالنسبة للمرحلة الأخيرة من المشروع فهي في المرحلة الختامية، حيث أننا لدينا عملية هارد فورك مقبلة، التي إذا لم تكن ملمًا بتقنية سلسلة الكتل، فسيكون هناك ترقية إلغاء توافق الإصدارات السابقة تمامًا. وهذا أمر مفروض، لأن البت كوين نشرت بعض

الترقيات لنظامهم حيث لا يكون بمقدورنا الاستخدام دون إلغاء توافق الإصدارات السابقة، وإننا نرغب في أن نبقى ملازمين للبت كوين.

وإننا نتطلع إلى العديد من الترقيات الأخرى، مثل جعل فترة انتهاء الصلاحية مناسبة بشكل كبير للمستخدم، وامتلاك أدلة عدم الوجود بالنسبة لجهات الاتصال لذلك يمكنك بكل سهولة إثبات ما إذا كان الاسم موجودًا أم لا، بالسماح لعقد نقطة الاسم بإسقاط البيانات القديمة للحصول على أفضل إمكانية توسع. وتظل التجزئات محتفظ بها بالتالي فالبيانات المسقطة لا يزال من الممكن إثباتها والسماح بشراء النيم كوين باستخدام البت كوين، أو ربما عملة Monero أو Zcash، دون وجود أي خطر من الطرف المناظر. ومعظم هذه الجهود قادها دانيال كرافت.

وأخيرًا أشكركم على توجيه الدعوة لي. ستسرني الإجابة عن الأسئلة.

ديفيد كونراد: حسنًا. شكرًا لك، جيريمي. لدينا بضع دقائق لتلقي الأسئلة وعرض الإجابة، هل لديكم أي أسئلة. نعم، ستيف.

ستيف كروكر: يا له من عرض تقديمي رائع. شكرًا جزيلاً.

جيريمي راند: شكرًا.

ستيف كروكر: لفت انتباهي إلى مستوى الحماية وما هي أنواع الأشياء التي يمكن أن تكون خطأ. وأن الحماية القوية تكون أي تغييرات تجرى وتكون معروفة، حسب فهمي لها الأمر. ولذلك ففي سيناريو تغيير منطقة الجذر، إذا كنا نستخدم ذلك، إذا – إذا قام أحد الأشخاص بتغيير شيء ما في منطقة الجذر، فسيكون الأمر معروفًا. وهو مستوى من الحماية ولكن هناك

مشكلة مختلفة تستجلب اهتمام بعض الأطراف وهي كيفية حماية إجراء مناوئ من نطاق المستوى الأعلى بحيث لا يمكن إتمامه في للتو. وربما بذور ذلك الأمر تنبثق في أن مفاتيح "M of N" المشتركة مع إمكانية أن الشخص العادي – الشخص الذي قد يقوم بتغيير في الغالب، سوف يعمل مفتاحه والمفاتيح الأخرى المنسجمة سوف تستخدم للتجاوز أو شيء من هذا القبيل. ولكنه لم يكن واضحًا 100% لي أن كل ذلك قد يحدث.

جيريمي راند: أجل. لذا، نعم، يمكنكم استخدام النيم كوين بكل تأكيد لغرض الوقاية من الهجمات الضارة على الإطلاق. وأشياء مثل طريقة التوقيع المتعدد وهي توقيعات "M of N"، يمكن أن تكون بكل تأكيد مفيدة لذلك. وبالمثل فالمثال الذي قدمته مع سياسة المصادقة الثنائية، يمكن أيضًا أن يستخدم لذلك.

لذا، حسنًا، أعتقد أنه يوجد حالات استخدام متعددة هنا. فحالة استخدام واحدة تؤكد أن أي شيء ضار يحدث يتم معرفته علنًا ولا يمكن إزالته من الذاكرة. ولكن نعم، أنتم على حق، فمن الضروري أن يكون بالإمكان محاولة صنع هجمات من الصعب أن تنجح في أول موضع قدر المستطاع. وحقًا، يمكن أن يساعد النيم كوين في ذلك. ونظرًا – نظرًا لأن نظام النيم كوين تم تصميمه في الأصل من أجل – المستخدمين النهائيين ممن لديهم اسم نطاق قياسي، وهي فكرة ستكون جيدة، فإذا ما كنت قلقًا أن أمين السجل الخاص بك قد يتلف اسمك بشكل ما، قد يسمحوا لشخص آخر أن يحدثه عرضًا، ومع النيم كوين، إذا كنت ترغب في ذلك، يمكنك أن تكون بنفسك أمين السجل. لذا، فأنت لا تحتاج إلى الاعتماد على طرف آخر، ما لم تكن ترغب – ما لم تكن تريد منهم أن يتم الاعتماد عليهم لحماية إضافية مثل التوقيعات المتعددة.

ستيف كروكر: يوجد عدد من الحالات حيث قد تحتاجون فيها إلى تدخل طرف آخر أو تخصيص الاسم في الموضع الأول أو استعادة المفاتيح إذا كانت قد فقدت أو الوقاية أو رد فعل لسلوك

مخادع وما إلى ذلك. وبالتالي، فإنني أتصور حدوث تغيير في النظام الذي لدينا حيث أنه لا يكون لديه دروب لهذه الأنواع من المعاملات، وبكل تأكيد، بمجرد أن تقوم بذلك، فإنك توضح أنك قد تتعرض لسلوك مخادع من المشغل الاستثنائي، ولذلك فإنها تكون – موضوع العثور على توافق جيد بينهم.

جيريمي راند: حسنًا. أجل. لذا، –

ستيف كروكر: حقًا، وهناك شيء آخر.

جيريمي راند: بالتأكيد.

ستيف كروكر: أما نوع المشغلين المخادعين الذين ننشغل بهم يجب ألا نشعر بالقلق على الإطلاق من كونهم مكتشفين.

جيريمي راند: حقًا، إنني أصدق ذلك بكب تأكيد، نعم. حقًا، فهناك خيار بكل تأكيد بين قدرة البشر على تقويم السلوك الضار الحادث مقابل قدرة – أي مستخدم شرعي مقتنع بأن البشر لا يمكنهم التسبب في تلف لاسمه الخاص به. وحقًا، يعد هذا الخيار أساسيًا. وليس هناك – ليس هناك طريقة جيدة للحصول على نوعي الحماية في الحال. فمن المحتمل أن يستبدل النيم كوين/ لهذا السبب، كليًا نظام اسم النطاق في أي وقت قريب. وفي الحقيقة، إنني أظن أن هناك عدد كبير من المستخدمين يفضلون نظام اسم النطاق على النيم كوين، لهذا السبب. ولهذا، هناك – أعتقد أن هناك أيضًا قاعدة مستخدمين ضرورية ممن يريدون – الخيارات

التي تعدها النيم كوين وأنهم يرغبون في احتمال – المخاطر، كما تعلمون، إذا ما سرق أحد الأشخاص مفتاحهم الخاص فقد قضي الأمر. لكن حقًا، فإنها بكل تأكيد مشكلة بحثية مفتوحة لكيفية توفير حماية لمفاتيحك الخاصة بطريقة جيدة حيث – يكون الخطر لا يستحق الذكر. وبالفعل، فإنها مشكلة بحثية مفتوحة.

ستيف كروكر: تعقيب سريع. قراءتي لتقنية اليوم هي أن سرقة مفتاح خاص أمر لا يستحق الذكر. أقصد أنكم تضعون ذلك في مجموعة من الأجهزة إذا ما نقلتموها بسرعة – غير أن الخيار يكون بأن لديكم خطر مرتفع جدًا حيث تفقدون التحكم إذا ما تم تدمير مفتاحكم الخاص أو فقده أو شيء من هذا القبيل. وبالتالي، فإن ذلك هو الإجراء الذي سيحتاج إلى استعادة.

جيريمي راند: أجل. إذا لم ينتابك خوف حيال طرف ضار يهم بأن يحصل على مفتاح لكنك تعتقد أنه يمكنك التأكد من – لكنك متخوف في الأساس أن مفتاحك قد يتم إتلافه عرضًا، ثم نعم. بالتالي، يمكنك أن تمتلك مفتاح احتياطي متاح. ويمكنك، على سبيل المثال، أن تمتلك سياسة توقيع متعدد التي تكون "1 ."N of، لذلك، يمكنك أن تمتلك نسخ احتياطية من "N" – آسف، نسخ احتياطية من N مطروح منها 1. وتعني "N1" أنه يمكنك استخدام المفتاح الأساسي لكل شيء، ويمكنك أيضًا استخدام سجل الوقت حتى يمكن استخدام المفاتيح الاحتياطية فقط لاستعادة الاسم إذا تم إتلاف المفتاح الأساسي وبعد ذلك، ستة شهور ولت. ولم يكن هناك وقت كافٍ لأن تنتهي صلاحية الاسم فضلاً عن إنشاءه، لذلك إذا حاول أي شخص أن يستخدم واحد من المفاتيح الاحتياطية بشكل ضار، فلا يمكنه استخدامه ما لم تفقد بالفعل المفتاح الأساسي أيضًا. ولذلك، نعم إنه نظام مرن إلى حد ما. ولكن بطريقة ما تحاول أن تعتمد على أن بعض أرقام المفاتيح لم يتم فقدها.

ديفيد كونراد: حسنًا. لدينا بضعة دقائق إضافية لطرح الأسئلة. آشا.

آشا هيمراجاني: نعم، شكرًا لك ديفيد. شكراً لكم على هذا العرض. علي أن أقول، إنني لم أحصل إلى حد ما على ثلاثة أرباع ذلك على الأرجح، وبالتالي هذا ما بسطه في خيالي ورغبت في رؤية ما إذا كنت قد حصلت على ذلك بشكل صحيح أم لا. وبالتالي، فهناك إحدى الطرق لتجنب الهجمات و– وبدلاً من – فبالتالي بدلاً من أن يتعرض اسم النطاق الخاص بك لخطر من حكومة ما أو اسم مسجل، يكون نظام اسم النطاق ساريًا للكمبيوتر الخاص بك، ويكون دفتر الهاتف الرقمي نوع من الكمبيوتر الخاص بك.

جيريمي راند: نعم.

آشا هيمراجاني: ومن ثم يضمن نوع البت كوين أن كل كمبيوتر في العالم يكون لديه نفس دفتر الهاتف الرقمي أو نفس نظام اسم النطاق، أيعد ذلك وصفًا عادلاً؟

جيريمي راند: نعم. نعم، أعتقد أن ذلك ملخصًا ممتازًا. نعم.

آشا هيمراجاني: حسنًا، رائع. يا للعجب. حسنًا. إنني أرغب، فيما بعد، أن أعود إلى ".BIT" الذي ذكرته آنفًا في الشرائح الخاصة بك. ويشير ذلك الآن إلى جميع مواقع الويب الخاصة بـ ".BIT."، هل هذا صحيح؟

جيريمي راند: نعم. نعم. تستخدم النيم كوين في الوقت الحالي نطاق المستوى الأعلى ".BIT"، وكنتيجة لذلك، إذا كان لديك برنامج نيم كوين مثبت فإنه سوف يواجه أي طلبات لنظام اسم النطاق لأي شيء ينتهي بنطاق ".BIT" وإنه سوف – يبحث عن هؤلاء باستخدام النيم كوين بدلاً من نطاق اسم النطاق.

آشا هيمراجاني: حسنًا. لدي سؤالان. لقد ذكرت أن نطاق ".BIT" غير مسجل مع ICANN. أيعد ذلك شرطًا؟ لذلك الأمر حتى يعمل.

جيريمي راند: إنه ليس شرطًا لذلك حتى يعمل على الصعيد التقني. أقصد أنه يعمل الآن بالرغم من أنه غير مسجل مع ICANN. أما الشغل الشاغل فهو، إذا منحت ICANN على سبيل الافتراض في المستقبل نطاق المستوى الأعلى ".BIT" إلى شخص ما آخر، فإنه لن يكون من الواضح بعد ذلك كيف من المفترض أن يعمل النظام. وبالنسبة للأشخاص الذين لديهم برنامج نيم كوين مثبت، كما هو مكتوب الآن، سوف يتمكنوا من الوصول إلى مواقع ويب النيم كوين باستخدام – هذا البحث، أما الأشخاص الذين ليس لديهم هذا البرنامج، سوف يتمكنوا من الوصول إلى كل ما فوضت ICANN نطاق ".BIT" لعمله. وبالنسبة للأشخاص الذين يحاولون الوصول إلى الآخرين لن يتمكنوا من القيام بذلك. وبالتالي فهناك خطر تعارض مساحة الأسماء بصورة أساسية. وهذا هو السبب وراء أننا نرغب حقيقة في أن نحاول الحصول عليه مسجلاً بصورة رسمية حيث لا يوجد أي خطر بأن، كما تعلمون، شخص ما قد يحاول أن يشتري نطاق ".BIT" من ICANN في المستقبل ويتسبب في حدوث مشاكل.

آشا هيمراجاني: حسنًا. إن كلمتك لها عظيم الأثر. شكرًا جزيلاً.

جيريمي راند: شكرًا.

ديفيد كونراد: حسنًا. كافيه

كافيه رانجبار: وشكراً لك، جيرمي، على العرض الذي قدمته. لدي سؤال سريع، لأنه على حد علمي أنك لم تعرض هذا الأمر على فريق عمل هندسة الإنترنت إلا في نطاقٍ ضيق من المناقشة. بالنسبة لاستخدام BIT. الخاص في التسجيل. هل كان ذلك الاختيار متعمدًا، أو هل تخطط لعرض هذا الأمر على فريق عمل هندسة الإنترنت أم لا؟

جيريمي راند: هذا سؤال وجيه. حسنًا، عندما تم تأسيس النيم كوين، الذي يعود إلى العام 2011 – وبالمناسبة، كان ذلك قبل انضمامي إلى نيم كوين – لم يكن المؤسسون الأصليون لديهم فكرة أن الاستخدام الخاص لأسماء التسجيل أمرًا موجودًا. وكان ردهم الأساسي، حسنًا دعونا فقط نأمل ألا تقوم ICANN – بتفويض BIT. لأي جهةٍ أخرى، وبالطبع كان هذا القرار غير حكيم جدًا ولكنهم لم يكونوا يعرفون بوجود مثل هذا الأمر.

وعندما حاولت المشروعات الثلاثة Tor، وI2P، وGanu.NET تسجيل نطاقات المستوى الأعلى الخاصة بها مؤخرًا عبر الاستخدام الخاص لأسماء التسجيل، سمعنا عن ذلك وقلنا أن الأمر يبدوا مناسبًا لنا، وتواصلنا مع المؤسسون بخصوص مسودة الإنترنت تلك، وقد قاموا بإضافتنا إلى تلك المسودة. ولكن للأسف تم تعليق مسودة الإنترنت هذه لأجلٍ غير مسمى لأسبابٍ سياسية لست أهلًا للتحدث بشأنها. وتم تمرير مسودة إنترنت جديدة وأصبح طلب الحصول على الملاحظات والتعقيبات متعلقًا بنطاق ONION. فقط وهو مشروع Tor. ومن ثم، أصبحت المشاريع الثلاثة الأخرى GanuNET، وI2P

ونيم كوين، نوعًا قيد انتظار التقدم الذي سيتم. ولكن نعم، لقد – شاركنا بنشاط؛ ربما لم تكن مشاركتنا بنفس القدر من النشاط المُفترض حدوثه. ولكننا بمجرد أن علمنا بوجود آلية يتوجب علينا اتباعها، بذلنا ما بوسعنا في محاولة اتباع تلك الآلية.

كافيه رانجبار: شكرًا جزيلاً.

جيريمي راند: شكرًا.

ديفيد كونراد: وارن ودانيل – في الواقع سنستمع إلى وارن ثم إليك، وبعدها سنغلق الدور – حتى العرض التقديمي التالي. وارن.

وارن كوماري: إن أحد الأمور التي تقلقني أن ملكيتكم كلها للنطاق مرتبطة بالمفتاح العام – عفوًا، بالمفتاح الخاص، وهناك العديد من الأمور الجذابة التي يمكنكم فعلها مثل M of N، وما إلى ذلك، ولكن المستخدمين يمرون بأوقاتٍ صعبة جدًا لفهم الكثير من هذه الأمور.

جيريمي راند: نعم، أنت على حق.

وارن كوماري: فمثلًا مع البت كوين، يمكنني أن أمتلك محفظتي الخاصة ويمكنني مواصلة تعقب جميع ما يخصني بنفسي، إلا أن هذه الأمور في غاية التعقيد بالنسبة لمعظم الناس، وبالتالي فهم يستخدمون محافظ الإنترنت ومن ثم يتم امتلاكها. فهل هناك عمل جارٍ لمحاولة تبسيط

الأمر على المستخدمين حتى يتمكنوا من فهم ما يفعلونه بالضبط في هذه الأمور وكيفية الحفاظ على المتعلقات داخليًا؟

جيريمي راند: نعم، هناك عمل جارٍ في هذا الشأن. وقد انهى موظفو البت كوين مُعظم هذا العمل وليس نحن، وذلك لأنهم يمتلكون الكثير من الموارد أكثر مما نمتلك. وقد تجدون المُنتج GreenAddress في عالم بيت كوين أكثر تشويقًا بكثير. وهو في الواقع يبدو مثل – إنها محفظة بيت كوين التي يمكنك إما تثبيتها كتطبيق الهاتف أو إضافتها كامتداد على المتصفح، أو شيء من هذا القبيل. ولكنها تعمل بغطاء مصادقة مكون من عنصرين. وما لم تحتاج فعليًا إلى استعادة مفاتيحك، وفي حالة – تلف خدمة المصادقة المكونة من عنصرين، فلا داعي للقلق حيال إدارة مفتاحك بنفسك، أو أمور مثل هذه. فالنظام يبذل ما في وسعه لتسهيل الاستخدام – قدر الإمكان. نعم، نود أن نرى أنظمةً مثل GreenAddress يتم استخدامها مع نيم كوين أيضًا.

ديفيد كونراد: حسنًا. ودانيال.

دانيال داردايلر: لديّ سؤالين. أولًا، بدأت حديثك بالقول أن الطريقة غير الحتمية لنظام اسم النطاق كانت تمثل مشكلة، ولكن لأي مدى تُعتبر مُشكلة؛ فكما تعلم، بمجرد أن تقوم بتسجيل اسمك، الذي يمر عبر أمين السجل والتسجيل، وبعدها يجب أن يكون حتميًا. هل هو محلل الاسم، والتخزين، وهل يعمل مثل بروتوكول نقل قاعدة البيانات. فأي جزء من مشكلة الحتمية الذي تحاول أن تجد له حلًا؟ هل هو التسجيل نفسه أم القرار؟ هذا هو سؤالي الأول.

أما التالي المتعلق بهذا الأمر، فهو السؤال عن الأداء. وما أعنيه، أن النظام قد تم إنشاؤه ليتميز بأداءٍ جيد جدًا بسبب وجود ملايين القرارات كل ثانيه، والنظام يستخدم

blockchain أو تسجيل إلحاق داخلي، أو عنوان IP دفتر الأستاذ العام، وعادةً – ما يتوجب أن تتولى هذه التسجيلات مساحة اسم النطاق بأكمله لإثبات أن هناك من يستخدم مفتاح التشفير، فكيف يعمل هذا الأمر؟ أقصد، بالنسبة للقيود المفروضة على الأداء وقيود تسجيل الإلحاق فقط.

جيريمي راند: أجل. أسئلة جيدة. بالنسبة لكون عدم الحتمية مشكلة، فإن المثال الذي ذكرته هذه الأيام هو، عندما تم تسجيل نص عنوان النطاق ly. في الأصل، ربما لم يتصور من قاموا بتسجيله أن النطاق ly. قد يتحكم به تنظيم داعش في المستقبل. حسنًا، الآن يوجد خطر حقيقي أن تنظيم داعش قد يكون المتحكم النهائي بذلك النطاق، فماذا سيحدث – إذا استطاعوا الاستيلاء عليه؟

هذا بالإضافة إلى أن أمناء سجلات النطاق، يرتكبون أخطاءً في بعض الأحيان. وقد أصبح هذا الأمر نادر الحدوث جدًا الآن، ولكن في السابق، كان أمناء سجل نظام اسم النطاق يقعون في خطأ تحويل أسماء النطاقات الأشخاصٍ آخرين بدون مصادقة مناسبة، كأن يقومون مثلًا بإرسال رسائل فاكس مزورة، أو أشياء من هذا القبيل.

لذا، لا أظن أن الأمر يشكل خطرًا قويًا جدًا بالضرورة في مجمل الأمر، ولكن يكفي الخطر المتمثل في أن الأمور قد تسير بطريقةٍ خاطئة، وأظن أن الأمر يستحق التدقيق في الأمور التي تسير بشكلٍ أكثر حتمية.

أما بالنسبة لإمكانية التوسع، فأنت محقٌ تمامًا في أن هياكل بيانات blockchains والمقتصرة على الإلحاق تكون اضعف بكثير في النطاق العام من أشياء مثل نظام أسم النطاق، لذلك أنت محقٌ تمامًا. وفي الحقيقة، لا يتضح في هذه النقطة تحديدًا إلى أي مدى يمكن أن يمتد نطاق نيم كوين. وقد كانت هناك مناقشة شيقة بخصوص هذا الأمر بالأمس خلال جلسة الأسئلة والأجوبة عندما كنت أنا ضمن اللجنة هنا. ولكن، نعم يمكن أن يمتد إلى نطاقٍ أوسع مما هو عليه الآن. وأظن أنه يمكن أن يتعامل مع معظم مستخدمي

خدمات نطاق ONION. بمشروع Tor بدون الكثير من المشاكل، وهو ما يُعد أمر مفيد جدًا. فهل يُمكن استبدال نظام أسم النطاق بالكامل في الوقت الحالي؟ بالتأكيد لا. هل يُمكن استبدال نظام أسم النطاق بالكامل في المستقبل البعيد؟ هذا أمرٌ يصعب البت فيه. فربما يُمكن، وربما لا.

ديفيد كونراد: حسنًا. شكرًا. أظن أننا متأخرون بضعة دقائق، لذا سيكون المتحدث التالي باول فيكسي من شركة فارسايت للخدمات الأمنية، ليحدثنا عن مناطق سياسة الرد.

تفضل يا باول.

باول فيكسي: شكراً لك ديفيد. ما دمنا نتحدث عن موضوع إضافة المزيد من طبقات التأثير الذي لا يقاوم إلى نظام أسم النطاق أو نظام التسمية بشكلٍ عام، لأنه لا يعمل بالشكل الذي نريده، فأنا أيضًا لدي ما أضيفه.

والنقطة التي أود الإشارة إليها، أن ICANN قد سجلت من قبل، وكذلك فعل العديد من المديرين التنفيذيين في أوقاتٍ عديدة، قولهم "نحن لسنا شرطة الإنترنت"، ودائمًا ما يكون هذا هو الرد على شخصٍ ما يرغب في أن يكون الإنهاء اكثر سهولة، لأنه سيكون هناك اسم نطاق في مكانٍ ما يُشير إلى بعض الموارد في مكانٍ ما، والتي تُسبب نوع من الأذى لشخصٍ ما، وكما تعلمون، كان الافتراض في عصر ما قبل الإنترنت يقول بأن كل شيء لابد أن تعود ملكيته لشخصٍ ما، وإذا كان هذا الشيء يُستخدم لأذيتك، فيمكنك أن تذهب – يمكنك أن تعرف من يكون هذا الشخص، وغما أن تقبض عليه أو تقاضيه أو على الأقل تُرسل إليه شكواك ليتصرف على أساسها.

لذا، فإن هذا الشيء الذي – لا أعلم ما هو – يتحمل الإنترنت المسؤولية عن تبييض خدمته، وتجد نفسك لا تنفك تطالب بإيقاف هذه الأشياء لأنها تؤذيك، وتصل في النهاية إلى أنه لا يوجد مالك لهذا الشيء، وتجد الجميع يقولون "أنا آسف، لا أعرف الشخص

الذي يتوجب عليك إيقافه لإيقاف هذا الشيء، ولكن لست أنا من يفعل ذلك"، فياله من أمرٍ مُحبط لأولئك الذين يتعرضون للأذى بسبب أشياء تحدث على الإنترنت.

لذا، فكما تعلمون، يمكن للمرء أن يشتكي من الجو المحيط به كما يشاء، أو يمكنه أن يصنع جوًا خاصًا به.

الشريحة التالية.

وأظن أن جميع الموجودين على يميني يعرفون هذا الأمر بالفعل، وجميع الموجودين على يساري يحتاجون إلى تذكير، لذا فمن أجل مصلحة جورج سادوسكي، دعوني أخوض في هذا الأمر.

[ضحك]

باول فيكسي: توجد ثلاث طبقات لتدفق بيانات نظام أسم النطاق.

لديك في الأسفل، مُحلل التعليمات البرمجية الخاص بك. فكل هواتفك الذكية، وأجهزة اللاب توب، والأجهزة، والأجهزة الافتراضية، وكل شيء يستعلم عن نظام أسم النطاق يُعتبر محللًا افتراضيًا. ويريد التحدث إلى خادم متكرر، وهو في الواقع ليس اسمًا جيدًا للغاية. وكنا نحتاج إلى قسمٍ تسويقي أفضل لهذا.

ولكن دعونا من نوع التكرار الذي نتحدث عنه، ولنتعامل معه وكأنه مساحة فارغة لكلمة. هذا الشيء مؤهل لمنحك الإجابة على أسئلتك، بما في ذلك الإجابة السلبية التي هي – لا توجد إجابة، أو اسم خاطئ، أو لا توجد بيانات أو مهما كانت الإجابة.

ويفعل ذلك باستخدام ذاكرة التخزين الموجودة هناك على اليسار، وبالتالي لدينا بعض التخزين. وعادةً لا يكون قرص تخزين كما هو ظاهر في الأيقونة هنا، ولكنه على الرغم

من ذلك يحفظ الأجوبة الحديثة، وبالتالي إذا سأل العديد من الناس عن نفس الشيء، فلست مضطرًا إلى الذهاب إلى الإنترنت وتكرار البحث مرات عديدة.

أما إذا سألك شخصٌ ما عن شيءٍ غير موجود في ذاكرة التخزين الخاصة بك، فسيتوجب عليك فعل ذلك. يجب أن ترتقي إلى المستوى الأعلى، ألا وهو أين تقع ICANN بالفعل. عالم ICANN، هو هيئة تفويض الخوادم. وخوادم اسم الجذر، وخوادم نطاق المستوى الأعلى، وخوادم نطاق المستوى الأعلى المؤثرة، والسجلات، وأمناء السجل، والمشتركون، جميعها تُسمى فضاء التفويض.

وبالتالي، فإن سلطة تفويض الخوادم، من وجهة نظر البروتوكول، هي المكان الذي يدخل فيه المحتوى إلى نظام أسم النطاق من الخارج. إذًا، فبمجرد أن يدخل المحتوى إلى نظام أسم النطاق، يمكنك الحصول عليه باستخدام بروتوكول نظام أسم النطاق، ولكن قبل أن تتمكن من جلبه، لابد أن يتم استيراده أولًا بطريقةٍ ما. وعادةً ما يتم استيراده من ملف نصي أو قاعدة بيانات أو أحد البرامج. وهذه هي وظيفة السلطات، أن تستورد محتوى نظام أسم النطاق من مصدرٍ خارجي.

ومن ثم، فإنه من غير الطبيعي في هذا العرض التقديمي في أحد اجتماعات ICANN، أن نُهمل الحديث عن سلطة تفويض الخوادم أو السياسة التي تُقرر من خلالها الاسم الذي ستنشئه أو من الذي ينبغي أن تشغله أو مهما كان. كما تعلمون – اعتدت في الغالب أن أتطرق إلى مثل هذه الأمور، وقد قضينا الكثير من الوقت في الحديث عن مسائل تدول حول سلطة تفويض الخادم والسياسة، وهذا تحديدًا ما تُنفق عليه جميع الأموال، ولكننا وعلى غير المعتاد سنتحدث عن الطبقة الوسطى.

والسبب في ذلك أن من يتعرضون للأذى بسبب استخدام الإنترنت، بوصفه المُسبب الرئيسي لهذا الأذى، يرغبون حقًا في التمكن من فعل شيء، وقد وصل الأمر إلى أنك لا يُمكنك منع من يرغبون في إيذائك من تسجيل أسماء نطاق ووضع محتوياتهم – المحتويات الموجودة على تلك النطاقات وتتسبب في إيذائك. وسيكون ذلك حلًا جذريًا.

فإذا ما تخيلت أنك في أحد الجهات على الإنترنت وهم في الجهة الأخرى، فسوف ترغب في حلٍ جذري يمنعهم، لا أدري، ربما من انتهاك علامةٍ تجارية على سبيل المثال، أو ملكية فكرية أو نشر مواد مسيئة للأطفال كأمثلةٍ أخرى. فلدينا جميع أنواع الأشياء التي قد تجدها مؤذية وتود لو أمكنك منعها من الوصول إلى الإنترنت على مستوى بعيد جدًا – جدًا، ولكنك لا تتمكن من ذلك بسبب وظائف الإنترنت باعتباره مسؤولًا عن تبييض الخدمة. وبالتالي، فإن ما نحن بصدده الآن، وهو ما ليس بعيد المنال ولكنه ليس ضروريًا، هو حلٌ شبه جذري؛ بمعنى، بما أنني لست قادرًا على منع إنشاء أسماء النطاقات هذه ولا أمتلك القدرة الكافية على إسقاطها، فيُمكنني تنظيم ما أطلع عليه بنظام أسم النطاق لأكون على دراية بتلك المحتويات لا إطار لها والتي تضرني مهما كانت.

وقد كان هذا ناجحًا للغاية. فقد بدأنا هذا المشروع عام 2011. وقد قمنا بمراجعة البروتوكول ثلاث مرات، وبالتالي فنحن بصدد البروتوكول 4 الآن. ونسعى في الوقت الحالي إلى وضع معيار البروتوكول الحالي، والذي سنقوم بعده بتسليم – تصنيف تغيير أدوات التحكم بالبروتوكول إلى فريق عمل هندسة الإنترنت، ولكن فريق عمل هندسة الإنترنت مهمته محدودة للغاية في الوقت الحالي.

وقد كان هذا حقًا نوعٌ من جهود فريق خاص، ولا يُشبه المشاريع ذات المصادر المفتوحة مثل نظام نيم كوين، وبالتالي فإن البعض منكم قد ساهم فعليًا بأفكارٍ ومميزات في هذا الأمر، ولكنكم لم تكونوا فريق عمل هندسة الإنترنت ولكننا نعتقد أنكم كنتم أذكياء واهتممتم بما قلتم.

ومن ثم، فإن ما نفعله هنا هو السماح باستخدام إشراف وتحليل من الخارج لسياسة العمل، وبعدها تتولى تلك السياسة تنظيم الردود، ولسوف آتي إلى النقطة "Z" خلال دقيقة، ولكن دعوني أوضح فقط أن ذاكرة التخزين لا تتأثر بهذا الأمر.

ويمكنكم تخيل سياسة تقول "انتبه، توجد خوارزمية توليد نطاق آلية جديدة، وهي ما تقوم بإنشاء كل هذه الأسماء. إنها مثل Conficker أو أيا كان. ونريد أن نتأكد من عدم وجود إجابة في حالة إذا أراد شخصٌ ما الاطلاع على أحد هذه الأسماء، لأن الإجابة – ربما

تُخبر أحد الروبوتات أو أحد العملاء المشبوهين على شبكتي بكيفية الوصول إلى أوامر التحكم بالخادم على شبكة شخص آخر ويجب عليَّ – مقاطعة هذا الأمر في مرحلةٍ ما. وأنا أختار أن أقاطعه في مرحلة نظام أسم النطاق".

وبالتالي، يمكنك القول، "حسنًا، إن هذه الأسماء، والأسماء القابلة للحوسبة التي يستخدمها الروبوت في الوقت الحالي، ممنوعة بالأساس"، وربما تكون هذه هي السياسة التي وضعتموها.

ولكن مستقبلًا، لن يكون هذا الأمر صحيحًا، أليس كذلك؟ فالمستقبل يأتي بمجموعة مختلفة من الأسماء. وهذه الخوارزميات الآلية لتوليد النطاق تستخدم التاريخ كجزء من طريقة حوسبة الأسماء التي تستخدمها. وبالتالي، ليس هنا جدوى من حظر الاسم طوال الوقت. وهذا الإجراء في الواقع – لا يفعل سوى زيادة احتمالية التضارب زيادةً كبيرة، فضلًا عن التضارب الموجود بالفعل في هذه الأسماء –

وتُشبه الخوارزمية الآلية لتوليد النطاق فيروس Conficker، حيث تقوم بتوليد أسماء قبيحة جدًا، ولكنها تتضارب مع ما أظنه أسماءً قبيحة ولكنها غير ضارة. ومن ثم تجد نفسك راغبًا في إزالتها.

لذلك، لم نضع السياسة في ذاكرة التخزين. ولكننا في الواقع نضع الحقيقة في ذاكرة التخزين.

لذلك لن تؤثر آلية سياسة الرد إلا على ما يراه محلل التعليمات البرمجية. ولا تؤثر على ما تم تخزينه أو ما تم جلبه من السلطات.

أخبرتكم أنني سوف أتحدث عن النقطة "Z" والنقطة "Z" هو الملف الذي يعكس حقيقة أن هذه الخوادم المتكررة موجودة بالفعل على الإنترنت. ويوجد منها 25 مليون خادم، معظمهم يجب ألا يكون موجود. فهي عبارة عن خطوط مودم غبية يجب ألا تشغل تلك الخدمة، ولكن هذا ما يحدث. ويوجد منها حوالي 2 مليون خط عالمي. وبالتالي، نحن

نتحدث عن 2 مليون خادم متكرر تقريبًا يهموننا. ومن ثم يوجد نظام أسم النطاق مفتوح و جوجل بعنوانهما 8.8.8.8. وهناك الكثير من الخوادم المتكررة المهمة. وجميعها – سأفكر في كيفية – كيف أريد قول ذلك؟

نريد أن نتمكن من التحكم في سياسة هذه الخوادم باستخدام بياناتٍ خارجية، والكثير من هذه الخوادم متعمقة داخل شبكاتٍ موجودة ومحمية بشكلٍ جنوني، فلا مجال لأن تصل إلى الخارج أو أن يصل إليها شيء من الخارج.

وهي تُعتبر آلية أمان جيدة لحماية أسماء الخوادم المتكررة الخاصة بك، حيث لا يمكن لمن هم خارج الشبكة أن يستخدمونها كوسيلة لهجمات الحرمان المنتشر للخدمة.

ولكننا لاحظنا أن الكثير منها تسمح بالتعامل خارج بروتوكول شبكة نظام أسم النطاق، وبالتالي قررنا أنه أذا أمكننا التسلل إلى السياسة في شكل – بيانات نظام أسم النطاق ليتم جلبها عبر المنفذ 53 لحزمة بروتوكول الإنترنت TCP، وهي الطريقة التي يتم من خلالها جلب بيانات نظام أسم النطاق الأخرى والتي يمكن أن تُفيد، فستكون هذه الخوادم المتكررة قادرة على الاشتراك في مصدر أحد السياسات. وعليه، تكون هذه هي بداية تجربة محاولة تكديس سياسة الرد في نموذج ملف نظام أسماء النطاقات.

وسيكون هذا الملف أقبح ملف لنظام أسماء النطاقات ستراه في حياتك. فهو مليء بالأنماط التي لا تحدث في العادة، وبالتالي فهو غير طبيعي إطلاقًا ومنظره مروِّع.

شيءٌ قد تكون فخورًا بمدى قبحه، إذا ما افترضت أن القُبح فنًا قائمًا بذاته.

ويتمثل سير العمل هنا في وجود شخصٌ ما أعلى اليمين يقوم بالمراقبة والتحليل. وأظنه قال، "حسنًا، روبوت جديد، أو عنصر جديد لتوليد البيانات، أو مجموعة أسماء جديدة لن يتم حلها اليوم"، أو لعله حجبٌ جديد لعنوان IP يستخدمه أحد مرسلي الرسائل النصية والبريدية غير المرغوب فيها، أو ربما حصلوا على محطة إذاعية لاحد القراصنة ويقومون بالإعلان عن مساحةٍ ما لبروتوكول BGP ليست ملكًا لهم، ونحن نريد حقًا أن

نتأكد أن أي إجابة قد تنتج عن تسجيل A أو تسجيل AAAA، داخل تلك المساحة المُقرصنة، لن يتم حلها اليوم.

ومن ثم، تقوم بتخزين نتائج تلك الملاحظة والتحليل مؤقتًا في ملف سياسة الرد، والذي يتم إدراجه فيما بعد في الطريقة العادية لتحويل الملف من خلال خوادم متكررة.

والآن، أود الإشارة إلى أن هذا التصرف يكون تطوعيًا. وسيرغب مُشغل الخادم المتكرر في تنفيذه. وهذا ليس مشروع قانون لمنع القرصنة. وليس شيئًا يفعله بك شخصٌ ما في مرتبةٍ أعلى ولا يُمكنك تجنبه.

والأكثر من ذلك، أنه إذا تم إشراك خادمك المتكرر في أحد هذه الملفات ولم يعجبك الأمر، فيُمكنك التحول إلى العنوان 8.8.8.8، وبالتالي فإن الأمر تطوعيًا للغاية حتى بالنسبة لمحلل التعليمات البرمجية. فالطريقة برمتها، بالرغم من إمكانية استخدامها لتنفيذ الرقابة، إلا أنها ليست كذلك. ويجب النظر إليها على أنها قيمة مضافة، أو على أنها لن تُستخدم من قِبل مُشغل الخادم المتكرر أو مُشغل محلل التعليمات البرمجية.

لذلك أود إخراج هذا أيضًا.

فما هي الأرقام إذًا؟ قد يكون أحد الخوادم المتكررة يعمل ببرنامج BIND أو Unbound، باستخدام برنامج ما أعرفه أو برنامج PowerDNS، أو – ويوجد برنامج رابع. توجد أربعة تطبيقات مستقلة لا تشارك أي رمز مصدر مع بعضها، وجميعها تعمل داخليًا بشكلٍ صحيح. في عالم فريق عمل هندسة الإنترنت، إذا كان لديك تطبيقات ذات قابلية تشغيل متعددة، فيمكنك الاعتقاد أن مستند البروتوكول مكتمل بشكلٍ كافٍ. لذا، أظن أننا تناولنا هذه النقطة مع النقطة الرابعة.

وهناك آلاف الخوادم المتكررة التي تشترك في ملف واحد أو أكثر من ملفات سياسة الرد. وهناك أيضًا العشرات من مزودي الخدمات الأمنية نشروا ملاحظاتهم وتحليلاتهم في هذا المنتدى. ويمثل رود راسموسين أحد هؤلاء، أو كان كذلك حتى عهد قريب.

ولكن هناك موقع ويب، dnsrpz.info، به قائمة بكل هذه التطبيقات، وقائمة بكل هؤلاء الناشرون، ويشتمل على مؤشرات بالمواصفات. وهذا ما يفعله المجتمع لحماية نفسه على المدى القريب من المشاكل التي تظهر على المدى البعيد ولا يمكننا منعها. وهي وسيلة فعالة. تعمل بشكلٍ جيد جدًا.

وتُقدم – شركتي الآن سياسة أمان في صيغة هذا الملف، وقد تلقت قبولًا جيدًا. وأظن أنها تحقق بعض النجاح مع رود أيضًا في شركته الحالية. وهي سياسة جيدة في المجال الأمني لأنها تأتي بالمزيد من العملاء لموظفينا، وهي جيدة أيضًا للأشخاص الذين يحاولون الدفاع عن أنفسهم، لأنها تمنحهم نقطة مراقبة جديدة على شبكاتهم ومعيارًا منفتحًا للغاية، بحيث يمكنهم امتلاك حلولًا من مقدمي خدمات متعددين يمكنهم من خلالها تحديد سياسات الأمان التي يريدونها.

وأخيرًا وليس آخرًا، إنها تمثل أيضًا حل للمؤسسات. فبالرغم من أنني أشرت إلى عملنا أنا ورود في مجال بيع هذه السياسات، إلا أنه من الشائع أيضًا أن يكون لدى البنوك، مثلًا، قائمة ببعض الأشياء التي لا يرغبون بحلها اليوم. وفي غياب هذه التقنية، تقوم المؤسسات بإنشاء ملفاتٍ فارغة ويضعون مساحة ضبابية صغيرة في أي نقطة من مساحة الاسم، التي يريدونها، لإخفاء البيانات ومنعها من الظهور. وإذا كنت تنفذ 6 ملايين منها وتقوم بانتهاك نصف هذا العدد يوميًا، فإن هذا يُعتبر عددًا مخيفًا من الانتهاكات التي تقوم بها في تكوين خادم الاسم الخاص بك. حيث أنك لا تغير تكوين خادم الاسم الخاص بك على شيء مثل ملف سياسة الرد. بل تغير فقط سياسة الرد. فهي عملية ليست مهمة على الإطلاق.

وبالتالي، لا شك أن أول ما يفعله من يقومون بالتثبيت، إنشاء ملف سياسة رد داخلي تقوم عليه شعبة الأمن الخاصة بهم حتى يكونوا على دراية بالتهديدات – ومرة أخرى، يتم الأمر عبر الملاحظة والتحليل، – ومن ثم يقومون بوضع سياسة رد سريعة على خادم الاسم المتكرر الخاص بهم على شكلٍ يشبه المصفوفة، وكأنك تضعها في مكانٍ واحد وتتفاجأ بتزامنها في كل مكان، ومن ثم تُصبح المؤسسة غير قادرة على إجابة أسئلة معينة أو تتوقف عن إجابة أسئلة قد ينتج عنها إجاباتٍ معينة.

وتنتهج سياساتٍ أخرى طريقة، لا تُجب على أي شيء إذا كان يتضمن خادم اسم معين. ومن ثم، يُمكنك تسميم محتوى جوهري دون معرفة السؤال أو الإجابة؛ ولكنك تعرف أنه قادم من اسم خادم اسم أو عنوان IP لخادم اسم في نطاقٍ معين، وبعدها يسوء الأمر. وهناك العديد من نقاط الارتكاز. وكما أخبرني ديفيد كونراد قبل ذلك، أننا لدينا ما يكفي من الحبال بحيث لو أراد أي شخص أن يشنق نفسه، سيتمكن من فعلها الآن.

وأظن أن الشيء الأخير الذي سيشير إليه معظمنا الآن هو قول "، أود أن أكذب"، وأتظاهر بعدم وجود شيء ما موجود بالفعل. وبعبارةٍ أخرى، هذه إشارة اصطناعية مزيفة لنطاق غير موجود. والنطاق غير الموجود، هو قيمة الرمز المرجعة في نظام أسم النطاق التي تشير إلى أن السؤال الذي تطرحه يعود إلى شيء غير موجود. ولكنه ليس بعيد تمامًا عن الشيء الوحيد الذي يمكنك فعله، لأن هناك الكثيرين ممن لا يريدون فعل ذلك. ولكن يرغبون في إنشاء ما يُسمى حديقة مسيجة، حيث – يمكنك، مثلًا، مشاهدة اسم Conficker، وروبوت Conficker بخوارزمية توليد نطاقات. وربما يكون ما تريده فعلًا وضع نافذة منبثقة على شاشتك مكتوب عليها "مرحبًا، أنت مصاب بفيروس Conficker". وبالفعل يمكنك فعل ذلك، إذا قمت فقط – بتقديم إجابة مستعارة مزيفة بدلًا من الإجابة بنطاق مزيف غير موجود لتقول أن الاسم المتعارف عليه لما تبحث عنه هو walledgarden.example.com. وهو نوع من خوادم الويب تشغله المؤسسة نفسها للتقول للناس "مرحبًا، ربما تكونون مصابون بفيروس، يجب الاتصال بقسم الدعم الفني حالًا". وهناك إجراءات أخرى كثيرة يمكنكم اتخاذها إلى جانب الكذب بشأن وجود شيء ما من عدمه.

وأظن فعلًا أن العنوان الأخير الذي يجب أن نشير إليه قبل الانتقال إلى الأسئلة والأجوبة هو، نحن كاذبون. فهذا كذب. فهذه السلطة مملوكة لجهةٍ ما تظن أنها تحمل برامج ضارة، وأنت لا تريد الحقيقة. وقد قررت أن تكذب على نفسك لأن الكذب هو الطريقة التي ستجعل بها شبكتك ومؤسستك تتجاوب مع تهديد معين. وعندما تكذب، تكون أحد الأشياء التي يتم انتهاكها هي الامتدادات الأمنية لنظام اسم النطاق. وتُعد الامتدادات الأمنية لنظام

اسم النطاق في غاية الأهمية بالنسبة لمستقبل اقتصاد العالم. ولابد أن نمتلكها، ليس فقط من أجل التحقق المستند على DNS للوحدات المسماة DANE ولكن أيضًا من أجل طلبات الوعي بالامتدادات الأمنية لنظام اسم النطاق التي تقابلنا في مراحل مختلفة. وهذا الكذب ينتهكها. فإذا استخدمت هذه الطريقة، وقامت سلطة التفويض بتوقيع البيانات نفسها، فسوف يتجاهلها الكود الخاص بنا. ولن يقوم الكود الخاص بنا بتطبيق السياسة على الأسماء الموقعة بالامتدادات الأمنية لنظام اسم النطاق. وهو ما سيمنح الأشرار فرصة سهلة جدًا للتسلل عبر كل هذا، فما عليهم سوى فتح الامتدادات الأمنية لنظام اسم النطاق.

ورغم ذلك، سيتوجب على مُحلل التعليمات البرمجية أن يطلب الامتدادات الأمنية لنظام اسم النطاق. ومن ثم، لا يوجد ما يكفي من الامتدادات الأمنية لنظام اسم النطاق لإبقاء ذلك بعيدًا عن التأثر. ولكنها ستمثل مشكل، في مرحلةٍ ما. ولدي توقع كامل أنه بعد أن ننشر المواصفات الحالية ونُحيل تغييرات التحكم إلى فريق عمل هندسة الإنترنت، سيظهر فورًا بروتوكول جديد يتطابق تمامًا مع هذا البروتوكول، بيد أنه سيكون أكثر حساسية بقليل مع الامتدادات الأمنية لنظام اسم النطاق. وهذه نقطة ضعف معروفة لا تؤثر علينا في الوقت الحالي. ولكنني أتمنى حقًا أن تؤثر علينا، لأنها إذا أثرت علينا فهذا يعني انتشار الامتدادات الأمنية لنظام اسم النطاق على نطاقٍ واسع، وهو ما نحتاج إليه. وهذه هي تعليقاتي التي حضرتها، وانا جاهز الآن للأسئلة والأجوبة. ديفيد، كم لدينا من الدقائق؟

ديفيد كونراد: ربما خمس أو سبع دقائق لطرح الأسئلة على باول. من يريد أن يبدأ؟

أليس لديك أسئلة لباول؟ حسنًا. حسنًا، سوف أبدأ.

[ضحك]

حسنًا يا بول، أظن أن أحد تطبيقات ملف سياسة الرد هو تعزيز المشكلة نوعًا ما، حيث أن الكثير من نطاقات gTLD الجديدة تتمتع بقبولٍ دولي. أولًا، هل هذا الأمر دقيق؟ وثانيًا، هل توجد طريقة للتعامل مع هذا؟

باول فيكسي: حسنًا، لدي ابن عمل بمجال اسم النطاق لفترةٍ من الزمن. وعندما أصبح النطاق ENTERPRISES.، قام بتسجيل VIXIE.ENTERPRISES وهو ما وجدته جيدًا لأنني كنت أقدم الاستشارات للشركات قبل أن يولد هو.

وبدأ في محاولة استخدامه واكتشف أن النطاق ENTERPRISES. لم يكن مجرد أحد الأنماط التي كانت تتوقع شركة كيونايتد إيرلاينز مثلًا، أن تربطه بحسابك. والآن أنا، ولحسن الحظ، أعرف الرجل بشركة يونايتد وتمكنت من إصلاح هذا الأمر. ولكنه كان واجه الكثير من المشاكل الأخرى. لذا، فهمت تمامًا أن هذه النطاقات العلوية يصعب استخدامها، لأن الكثير من الناس يظن أن النطاق قد يكون COM. أو NET. أو ORG. أو INFO. أو مجموعة من أكواد الدولة. وإذا لم يكن كذلك، فلابد أنه خطأً في البناء اللغوي. وبالتالي، أدركت ذلك. ولكن هذه المشكلة ليست بسبب ملفات سياسة الرد، ولم أسمع من قبل أن هذه المشكلة لها علاقة بملفات سياسة الرد.

ديفيد كونراد: حسنًا. لقد أشرت إلى أن ملفات سياسة الرد لا تعمل مع الامتدادات الأمنية لنظام اسم النطاق. وأنا أفترض أن ملفات سياسة الرد قد تعمل مع الامتدادات الأمنية لنظام اسم النطاق إذا كان الملف موقعًا، وتمت إعادة الرد ليتم التحقق منه، وأن الملف فعلا يمكن التحقق منه. وبعد التحقق، قد يتم تعديل الإجابة التي تمت إعادتها إلى مُحلل التعليمات البرمجية على نحوٍ مناسب حسبما أشار ملف سياسة الرد.

باول فيكسي: هذا صحيح تقريبًا. فلا شك أن الأمر يسير على هذا النسق ما لم تطلب المعالجة الامتدادات الأمنية لنظام اسم النطاق. فإذا لم تقم بضبط D.O. يساوي 1، فإن ما قلته لتوك هو ما سيحدث. فسوف نجلب البيانات. وسوف نتحقق منها، إذا كان ذلك ممكنًا. وسوف نضعها في ذاكرة التخزين. وبالتالي فإننا عندما نحاول طرح إجابة للسؤال الأصلي، ستجدنا نقول، انتظر فنحن لدينا سياسة. والمعالجة لم تطلب الامتدادات الأمنية لنظام اسم النطاق، لذا فنحن بصدد – إيقاظ الموظفين، لأن المعالجة إذا لم تتمكن من إخبارنا أننا نكذب، فسوف نكذب. وبالرغم من ذلك، إذا طلبت المعالجة سجلات نظام أسم النطاق وكان لدينا سجلات نظام أسم النطاق، فلن نطبق السياسة.

ديفيد كونراد: جورج؟

جورج سادوسكي: شكراً لك، يا باول، على التذكِرة. أنا تقريبا على استعداد لإجراء الاختبار.

لذا، أعتقد أن هذه المسألة تتعلق أكثر بالأشخاص الذين ينتجون المعلومات التي تستند إليها السياسة.

تحدث عن اعتبارات فترة بقاء البيانات في الحاسوب أو في الشبكة هنا. كم مرة يتعين عليك بث هذا؟ ما مدى تكرار التغيير الذي تريد تقديمه للمستخدمين؟ كيف تعرف ماهية فترة بقاء البيانات في الحاسوب أو في الشبكة؟

باول فيكسي: حسنًا. صدق أم لا، أنا سعيد أنك سألت. الاتصال مباشر. لذلك، – إذا قمت بإجراء تغيير، فلأن هذه منطقة ملف نظام أسماء النطاقات عادية، سيكون هناك إخطار وسيكون هناك نقل منطقة إضافية، وستكون هناك تحديثات فورية تقريبًا. لذلك، فبقدر ما تقوم بتغيير رأيك وتقول، أنا أحب هذه السياسة قبل عشر دقائق ولكن أنا لا أحب ذلك الآن، يمكنك

فقط تغيير فكرك وهو ما سينعكس على الفور عبر قاعدة المشتركين خاصتك. من المهم جدا بالنسبة لنا أن لا نكسر أي شيء جديد. لذلك، لتحقيق هذه الغاية، إذا – نحن لا نريد أي بيانات قديمة في النظام. وسوف أعطيكم مثالًا.

تبيع شركتي خدمة نطاق تمت مراقبتها حديثًا. وذلك لأننا لاحظنا أن هناك 2 2/1 نقطة تفويض جديدة يتم إنشاؤها في الإنترنت كل ثانية، وربما سيختفي نصفها في غضون 24 ساعة. وسيختفي 6/1 منها في غضون عشر دقائق. وهناك معدل خضخضة عالٍ جدًا. يتم إنشاء هذه الأشياء لغرض إزعاج شخص ما، ويتم إنهاؤها على الفور تقريبا في كثير من الحالات أو سيتم وضعهم على القائمة السوداء من قبل جهات مثل SpamHaus. وهذا لا يعني أن كل ما هو جديد هو سيء، ولكن هذا يعني أن هناك احتمال إحصائي بأن يكون الشيء الجديد سيئًا.

منذ أن أتذكر الأيام الخوالي الجيدة حيث كان يمكنك أن تطلب اسم COM. وإذا كان ذلك بعد يوم الثلاثاء، سوف تحصل عليه يوم الجمعة، أنا راضٍ أسماء نطاقات جديدة لا تعمل بهذا الشكل الجيد. كل شيء أن ICANN ونظامها الإيكولوجي قد خفضت زمن الحصول عليه إلى 30 ثانية شريطة ألا يكون لديها حقا حالة استخدام غير ضار والتي أود أن يتم الاهتمام بها.

لذلك، هذا يعني أننا يجب أن نرسل تحديثًا مرة واحدة في الثانية لمشتركي RPZ لدينا قائلين: "هذه هي أسماء النطاقات الجديدة التي راقبنا. وبالمناسبة، نحن الآن نحذف تلك التي تتجاوز العشر دقائق لأنك تريد فقط أسماء جديدة ولكنها ليست جديدة بعد مضي عشر دقائق، حسب التعريف الخاص بك. " لدينا تعريفات مختلفة.

تستطيع الشبكات التي ترسل التحديث مرة واحدة في الثانية مزامنة سياسة الاستجابة عبر الآلاف من العملاء الاصطناعيين أو العشرات من العملاء الفعليين. وهذا يجدي نفعًا. وبسهولة ويسر. فلا يوجد تأخير.

ديفيد كونراد: وارن؟

وارن كوماري: لذلك، أعتقد أن هذا تعليق أكثر من كونه سؤالًا. اعتدت على تشغيل خادم الأسماء الخاص بي لعدد من النطاقات، وبعد ذلك حصلت على إزعاج حقا مع كمية من البريد غير المرغوب فيه لذلك سأضطر إلى إيقافها.

وبعد ذلك بدأت الاشتراك في رسائل RPZ من مجموعة مختلفة من الناس، ولقد شغلتها كلها مرة أخرى لأنه مع RPZ، لم يكن لدي تقريبا أي بريد غير مرغوب فيه للتعامل معه، أليس كذلك؟ أحصل على رسائل البريد المزعج من عدة أشخاص مع RPZ. إنها تراعي فقط الأشياء المهمة، والآن كل شيء يعمل مرة أخرى. هذا...

باول فيكسي: شكرا لقولك هذا. واسمح لي أن أعلق على تعليقك.

لا يمكنك إنجاز أي عمل على الإنترنت ما لم يعمل نظام اسم النطاق. أعلم أن هناك الكثير من بروتوكولات النظير للنظير، حتى أن مستخدمي BitTorrent لا يلاحظون عندما لا يعمل نظام اسم النطاق. ولكن بالنسبة للبقية منا، إذا كان نظام اسم النطاق لا يعمل، لا يهم ما يمكن الوصول إليه لأننا لن نكتب عناوين I.P. ولن نكتب بالتأكيد عناوين IPv6.

والآن، أصبحت الملكية تعمل للأشرار أيضًا. ليس الأخيار فقط الذين لا يستطيعون إنجاز الأعمال إذا لم يعمل نظام اسم النطاق. فلن يمكن الوصول إلى الأشرار إذا لم يكونوا في نظام اسم النطاق.

وبالنسبة لي، لقد أتيت على ذكر البريد غير المرغوب فيه. بالنسبة لي، هذا يعني إغلاق البريد الإلكتروني المزعج.

لقد حصلت على البريد الخاص بي، إنها Postfix وهي موصلة عبر الأسلاك وهي تحاول إجراء بحث نظام اسم النطاق في كل اسم بالعنوان، وكل اسم في المغلف، وكل اسم في المتن. وإذا فشل أي منهم، فإنني أرفض البريد، وهو ما يعني أن استخدام هذه

النقطة المختلطة كمجرد مكان لقول هذه الأسماء يجب أن تكون غير موجودة، إذا كانت موجودة، ثم كُذِب في ذلك وقيل أنها لا توجد، وسوف يسبب كل شيء أنواع مختلفة من الإخفاقات الأخرى التي تحدث داخل البنية التحتية الخاصة بك. فعليك أن تكون مستعدًا لها. يمكن أن يكون من المستغرب قليلا عندما كنت لا تحصل على هذا البريد المزعج. في الواقع، ما قلته هو القصد الثانوي من هذا الجهد كله.

ديفيد كونراد: حسنًا. شكرا لك، بول، على حديثك عن RPZ، والآن ننتقل إلى بول ووترز.

بول ووترز: شكرًا.

بما أن لدي الميكروفون، تعليق صغير. لا بد لي من القول بأن بول فيكسي وجون جيلمور هما أكثر الأشخاص صعوبة في التواصل معهم عبر البريد الإلكتروني على كوكب الأرض بسبب كل ما لديهم من دفاع أو عدم وجود آليات دفاعية ينشرونها بشكل أساسي.

لذلك، وبما قيل –

>> (بعيدًا عن الميكروفون.)

بول ووترز: أنا راضٍ بالأضرار الجانبية.

لذلك، لنشر الامتدادات الأمنية لنظام اسم النطاق على نطاق واسع، ثمة مشكلة. يسجل DS أن الأشخاص بحاجة للوصول إلى منطقتهم الأم، إنها عملية صعبة للغاية لخوضها على وتشمل الكثير من الأشخاص، وأهم شخص يعمل في المسجل لا يعرف أي شيء حقًا. فقد اشترى خدمة واسم نطاق للتو ولا يعرف شيئًا. هو يرغب فقط في أن تعمل الخدمة وأن يملك مشغل نطاق يدير كل شيء نيابة عنه، ومن ثم فهو لا يعرف حتى ما

هو الامتدادات الأمنية لنظام اسم النطاق ولا يعرفون كيفية تمكينها، حتى لو كان مشغل نظام اسم النطاق يخبره بما يفعل، فتقابله صعوبات جمة في اتباع التعليمات.

لذلك، هناك الكثير من النطاقات المختلفة – مقدمي خدمات استضافة كبيرة جدا التي وقعت أساسا ولكن لم تفوض مع سجل DS، لذلك على الرغم من أنها آمنة في حد ذاتها، إلا أنها معزولة لأن – سجل DS لم يذهب إلى الأصل لأنه لا توجد وسيلة للقيام بذلك.

وهكذا، فإن هذه المشكلة تحتاج إلى حل.

وقد تخلى فريق عمل هندسة الإنترنت أولا عن معالجته، ولكن في مرحلة ما، أصبح مشكلة كبيرة جدًا، لذلك عادوا وهم الآن مرتبكون. سأغلق فقط جهازي المحمول.

لذا، فإن الأمرين اللذين يلزمهم القيام بهما – وهذا يتم الآن في RFC–8078 الذي تم نشره للتو الأسبوع الماضي – هو أنهم يحتاجون إلى أن يكون لديهم طريقة كي يرسل مشغل نظام اسم النطاق إشارة إلى السجل بأن هذا النطاق الآن لديه سجل DS، ويمكن نشره في سجل DS هذا.

ومن ثم، فإن الأمر الآخر الذي يحتاج مشغلو DS أيضا هو أن يقول إن "زبائني يبتعدون؛ ولا يريد العميل الامتدادات الأمنية لنظام اسم النطاق بعد ذلك". نحن بحاجة إلى بعض الطرق لإخطار السجل بإزالة ذلك السجل مرة أخرى، وكذلك عندما لا تكون هناك حاجة إلى الامتدادات الأمنية لنظام اسم النطاق.

وهكذا، فإن طلب الحصول على الملاحظات والتعقيبات هذا يسمح أساسًا بذلك. ماذا يفعل؟ هل يتم إنشاؤه؟ – يستخدم زمن التسجيل CDS، وهو في الأساس نفس نوع السجل مثل DS ولكن يتم نشرها على جانب العميل، وذلك في منطقة العميل نفسها.

وهكذا، بمجرد نشرها هناك، تجد طريقة للوصول إلى السجل الخاص بك ويقول "مرحبا، لقد نشرت سجل CDS هذا. أيمكنك إلقاء نظرة على ذلك، وإذا نال موفقتك، يتم نشره كسجل DS في منطقتك الأم."

وهكذا، هذا ما يفعله هذا السجل الجديد.

عذرًا. السجل لا يفعل ذلك. استخدامه هنا هو الجديد.

هناك طرق مختلفة لكيفية الاتصال بالسجل الخاص بك، ويترك هذا إلى المسودات الأخرى. يوجد حاليًا مسودة قيد التنفيذ، على سبيل المثال، باستخدام واجهة مريحة، وذلك باستخدام بروتوكول نقل النص التشعبي، لنقل تلك المعلومات، ولكن يمكن للأشخاص ابتكار آليات أخرى لذلك أيضًا. وعندئذ يكون سجل التعطيل الخاص هو سجل CDS مع جميع الأصفار، والتي تعني في الأساس، "يرجى تعطيل هذا، نحن لا نريد أي شيء."

وهناك في الواقع خطأ مطبعي على الشريحة. يجب أن يكون هناك صفرًا رابعًا، وهو أيضا مسألة في التنقيح الأخير للمشروع، ولكننا لم يُلتقط في الوقت المناسب لمنشور طلب الحصول على الملاحظات والتعقيبات ولكن من الواضح، لم أحدث الشريحة خاصتي.

ولهذا فإن هذا النظام مجدٍ. وبسبب أن هناك أيضًا امتدادات بروتوكول تزويد مرن جديدة الآن، بمجرد أن يقبلوا هذا النوع من التحديث خارج الحدود من مشغل نظام اسم النطاق، يمكنهم الإشارة إلى ذلك مرة أخرى إلى أمناء السجلات بحيث يدركون أيضا أن هذا السجل قد تم تحديثه و لم يأت من خلال مسار بروتوكول تزويد مرن تلقائي.

ويجري حاليا نشر ها أو في مرحلة النشر لعدد من نطاقات TLD، وسرعان ما يعني ذلك أن هناك مئات الآلاف من النطاقات الموقعة الأخرى للامتدادات الأمنية لنظام اسم النطاق المفوضة، ومن ثم ينبغي أن يكون هذا قفزة كبيرة في نشر الامتدادات الأمنية لنظام اسم النطاق، ونأمل أن تحقق نجاحًا جيدًا.

ديفيد كونراد: حسنًا. هل توجد أي أسئلة لبول؟

نعم، ليمان

لارس–جوهان ليمان: ليتفضل لارس ليمان استيضاح بسيط. هذه هي سجلات CDS كما اقترحها – هل كان أولاف كولكمان؟ أم السجلات التي كانت توزع في فريق عمل هندسة الإنترنت؟

بول ووترز: أجل. هذا هو طلب الحصول على الملاحظات والتعقيبات من قبل أولاف كولكمان، أعني، نعم.

لارس–جوهان ليمان: حسنًا. شكرًا. وأيضا، هذا النوع يصب القليل من التركيز على عدم وجود علاقة رسمية بين مشغلي نظام اسم النطاق والسجلات، وأعتقد أنه أمر جيد.

بول ووترز: لم أذكر هذه الكلمة عن قصد.

ديفيد كونراد: باتريك؟

باتريك فالتستروم: هل كنت تلقي نظرة على –

إلى يسارك هنا.

[ضحك]

باتريك فالتستروم: لذلك، ما حدث في الحالة العادية – إذا كنتم ستعودون إلى الشريحة، من فضلكم.

في الحالة العادية، فإن معاملة الامتدادات الأمنية لنظام اسم النطاق تسير عبر أمين السجل، لذلك يتحمل أمين السجل المسؤولية النهائية للولاية لضمان إكمال كل ما يتعلق بالمشترك، بما في ذلك المفتاح – المادة الرئيسية.

في هذه الحالة، يتم تحديث المفتاح من مشغل نظام اسم النطاق إلى السجل دون تمرير أمين السجل، حسنًا؟

بول ووترز: هذا صحيح.

باتريك فالتستروم: وما تقوله هو أن يتم تشغيل هذا من خلال حدث في بروتوكول التزويد المرن، أليس كذلك؟

لذلك، من المفترض أن يقوم أمين السجل باستخدام الأمر وسحبه في هذه الحالة لجلب المعلومات حول المواد الرئيسية الجديدة.

هل هذا هو الغرض؟

ما أشعر بالتوتر إزاءه حقًا هو أن أمين السجل لا يملك فجأة رؤية كاملة بشأن المنطقة، وهذه هي المسألة الذي قد يكون لها تأثير على مسؤوليات أمين السجل فيما يتعلق بالسجل.

بول ووترز: هذا صحيح. نعم. ولكن كان فهمي أن هناك امتداد بروتوكول تزويد مرن جديد يسمح للسجل بالدفع، وهذا ليس معناه أم أمين السجل بحاجة إلى السحب.

باتريك فالتستروم: بالتأكيد. هناك امتدادات حيث يمكنك القيام بذلك. ولكن هناك – في تصميم بروتوكول التزويد المرن العادي، يكون التصميم كله معدًا لأمناء السجلات لتحديث التسجيل وليس العكس.

بول ووترز: هذا صحيح.

باتريك فالتستروم: حسنًا. هذا هو شيء آخر حيث يكون التسجيل يصف تغييرًا في آلة الحالة في أمين السجل، ولدينا عدد قليل جدا من تلك، وهذا هو واحد آخر، أليس كذلك؟

بول ووترز: حسنًا. ومع ذلك، يستطيع أمين السجل أيضًا أن يدعم نفس الآلية وبعد ذلك يتحدث المشترك معهم.

لذلك، بالنسبة لأولئك الذين يرغبون في تنفيذ جميع متطلبات الامتدادات الأمنية لنظام اسم النطاق التي لا تحتاج إلى هذا العمل، لن يحتاجون إلى عمل آلية الحالة. طالما أن أمين السجل ومشغل نظام اسم النطاق لديهما علاقة عمل جيدة حيث يمكنهما التحدث مع بعضهما البعض. لأنه إذا كان أمين السجل لا يستطيع التحدث إلى مشغل نظام اسم النطاق، تبقى المشكلة أنها لا يمكن الحصول على هذه المعلومات ما لم تستخدم هذه الآلية.

باتريك فالتستروم: يمكنني التحدث معك باستخدام استعلام نظام أسماء النطاقات، أليس كذلك؟

على أي حال، من أجل الشفافية، عندما راجعت هذه الوثيقة، اقترحت أن تكون هذه الوثيقة – يجب أن توحد سجل CDS الممتاز هذا بصفة مستقلة عما إذا كان السجل أو أمين السجل الذي يسحبه.

بول ووترز: أين سينشر أمين السجل هذا؟ هل تقصد إذا كان أمين السجل سيرسلها من خلال بروتوكول التزويد المرن؟

باتريك فالتستروم: لا يوجد نشر – أمين المسجل يجلب DS الجديد من مشغل نظام اسم النطاق ويدفعه إلى التسجيل باستخدام بروتوكول التزويد المرن.

بول ووترز: ويمكنهم أن يفعلوا ذلك من دون هذا المشروع.

ديفيد كونراد: لذا، –

باتريك فالتستروم: دعونا نناقش هذا خارج الخط. أجل. لقد سبق أن أوضحت ذلك على القائمة البريدية لفريق عمل هندسة الإنترنت وربما لا يتعين علي القيام بذلك هنا مرة أخرى.

ديفيد كونراد: حسنًا. دان، ثم وارن.

دان يورك: كنت فقط سأقول شكرا لك، بول، على تقديم هذا، وأعتقد أن النقطة الأساسية ربما لأعضاء مجلس إدارة ICANN والأشخاص الآخرين الذين يستمعون هنا والذين لا يرغبون في الغوص في تفاصيل هذا هو مجرد إدراك أن هذا جزء من العمل الجاري لتوفير إمكانية

أفضل في الطريقة التي تعمل بها الامتدادات الأمنية لنظام اسم النطاق لأننا نظرنا في النشر على نطاق واسع للامتدادات الأمنية لنظام اسم النطاق من قبل مشغلي نظام أسماء النطاقات أو من أشخاص آخرين يبحثون عن محاولة القيام بهذا، واحدة من الحواجز الكبيرة التي تم تحديدها في الحصول على هذه المعلومات، سجلات DS هذه، حتى السجلات.

وحيث إن هذه إحدى الآليات التي هي متاحة الآن للسجلات التي تختار الاستفادة هذا للمساعدة في التشغيل الآلي لهذا المنشور المعلوماتي، وجعل هذا أفضل مما سيؤدي إلى نظام اسم نطاق أكثر أمنا في نهاية المطاف.

لذلك، هذا هو – هذه حقا النقطة الرئيسية للخروج من هذا، إنها آلية جديدة متوفرة الآن وحتى السجلات يمكن أن تنظر في هذا كوسيلة لإنجاز هذا العمل.

وبالنسبة لنقطة باتريك، يمكن لأمناء السجلات النظر إلى هذا أيضا.

ديفيد كونراد: وارن؟

وارن كوماري: لذلك، السبب في أنني بدأت في محاولة لمقاطعة باتريك هو أعتقد أن الناس يتحدثون في أغراض مشتركة.

وأعتقد أيضا، لارس، قلت أن المشروع أصلا Olaf. إنه في الواقع Olafur، أعتقد أن هذا هو الاسم الأصلي – نعم. أفعل هذا أنا وOlafur. أجل.

لذلك، فإن المستند الأصلي لم يكن لديه القدرة على إيقاف الناس عن نشر هذه السجلات تلقائيًا. كان عليك أن تمر من خلال التسجيل أو أمين السجل، والذي أعتقد أن هذا ما كان باتريك يتحدث عنه. لقد تركن على وجه التحديد "جزئية "يمكنك تجاوز أمين السجل

خاصتك" بسبب الشواغل نفسها التي ذكرها باتريك. وهذا يبني على المشروع القديم ويضيف ميزات جديدة. أو ربما أكون قد أسأت فهم –

باتريك فالتستروم: ما أحاول فعله هو مجرد فصل الميزة التقنية، وهي قدرة مشغل DNS على الإشارة إلى أن هذه هي المادة الجديدة من تأثير السياسة المحتمل بشأن العلاقة بين المشترك وأمين السجل والسجل. هذه المناقشة مختلفة تمامًا وربما تجدون فوضوي في نطاقات TLD معينة.

ديفيد كونراد: هل لي بتعليق بسيط؟ أجل.

>> باتريك، المشكلة الأساسية التي تحتاج إلى حل هي اكتشاف من هو المشترك، ومن يستطيع التحدث معه. لدينا عدد محدود من السجلات لذا فهي مريحة كنقطة انطلاق للحديث، ولكن إذا كنا نستطيع نحو ما الوصول إلى RDAP أو أي بروتوكول آخر، والعثور على نقطة دخول إلى الكيان الذي هو على استعداد للتحدث معنا، ويفضل أن يكون السجل أو التجزئة ، حتى، أو من موزع موزع، وهذا هو الشيء لا أحد يستطيع أن يجده اليوم.

ديفيد كونراد: ديمتري؟

ديمتري كوهمانويك: مرحبًا. أريد فقط أن أدي بتعليق سريع عن سبب تضاعف صندوق التسجيل. أعتقد أنه خطأ كتابي. ثانيًا، أود أن أؤيد التعليق الثاني لباتريك فالتستروم في ذلك، نعم، ونموذج بروتوكول التزويد المرن – وأنا، بالمناسبة، أمثل واحد من نطاقات TLD، وهو نطاق المستوى الأعلى لرمز البلد. نحن ندير بروتوكول التزويد المرن إنها أوكرانيا. أعتقد أن

النموذج عندما تكون الحالة منقسمة يكون سيئًا للغاية. كما أعتقد أن نموذج السحب سيئ للغاية ولا يزيد. ومع ذلك – نعم، يدعم بروتوكول التزويد المرن تحديثات DS، ولكن أكبر مشكلة هنا هي أننا نحاول فصل DNS – آسف، إدارة سجل NS وسجل DS. وهذا سيء. لأن تغيير مشغل DNS قد ينطوي على حد سواء تغيير سجل DS وسجل DNS. ويبدو من الغريب أنه يُفترض بتحديثات DS ألا (تدرك) هذا المشروع دون الإشراف على سجل DNS.

لذلك، أود أن أقول أن نعود إلى مجلس الرسم ونرى كيف يعالج هذا الفصل الكامل لسجل، مثلا، تحديث البيانات عن أسماء الكيانات والعناوين والأشياء مقابل البيانات التقنية. نعم، إنها فكرة جيدة لتفقد المشغل الفني الخارجي، ولكن النقطة هو الحل الخاطئ، بالإضافة إلى عدم وجود علاقة تعاقدية بين مشغل نظام اسم النطاق، واحد أو اثنين، والتسجيل هو الحل الخاطئ، وهذا ليس وسيلة للحل أو جعل الإنترنت أكثر أمانًا.

لذلك، نعم، محاولة لطيفة، ولكن أود فقط –

بول ووترز: لذلك، وسوف أكون فقط – ملاحظة سريعة جدًا وبعد ذلك سوف أعطي الكلمة لبول فكسي.

كان هناك نقاش طويل في فريق عمل هندسة الإنترنت عن المشغلات مقابل الموقتات، وذلك دعونا لا نكرر ذلك مرة أخرى.

ويوجد خيار يقضي بأن السجلات يمكن أن تحدد الاختيار، وإذا كان يتعذر على بعض السجلات تعاقديًا أن تفعل ذلك أو لا تريد أن تفعل ذلك، وهذا شيء طيب، ولكن سيكون هذا خيارًا يمكن أن يكون مفيدًا لعدد كبير من الناس الذين لا يمكنهم حاليًا دفع سجلات DS إلى حيث يفترض بها.

ديمتري كوهمانويك: حسنًا، نعم. توج مشكلات عديدة. ولا أعتقد أننا يجب مناقشة هذا هنا. فمن الأفضل أن يتم ذلك في بيئة فريق عمل هندسة الإنترنت. شكرًا.

بول ووترز: حسنًا.

ديفيد كونراد: بول؟

باول فيكسي: كنت سأركز على هذه النقطة. تعمل لجنة الترشيح بغاية الجد للحصول على الأشخاص الأكثر تأهيلًا واستعدادًا للعمل في هذا المجلس، وهم ليسوا بالضرورة فنيين مثل الأشخاص الذين كانوا يستخدمون الإنترنت في السنوات التي سبقت وجود ICANN. يجب علينا أن نستخدم الوقت بحكمة واحترامهم وقتهم، لذا فالرجاء النزول بحججك إلى مستوى يمكن لجورج سادوسكي أن يفهمه.

[ضحك]

ديفيد كونراد: وبذلك، نحن الآن في أي عمل آخر.

كما تعلمون، كانت هذه محاولة لإعادة هيكلة الطريقة التي تعمل بها TEG. قدمنا إحاطات، من صفحة أو صفحتين إلى أعضاء المجلس قبل الاجتماع وأتساءل فقط إذا كان ذلك مفيدًا أم ينبغي لنا مواصلة محاولة تطوير TEG بطريقة تجعل ذلك أكثر فائدة لأعضاء المجلس.

ويمكنكم إما القول الآن أو مراسلتي عبر البريد الإلكتروني أو التحدث معي في حفل الكوكتيل الذي سيقام لاحقًا. ستغادر الحافلات في غضون 15 دقيقة. وبذلك، نصل إلى ختام دورة TEG هذه، وأشكركم على مشاركتكم.

[تصفيق]

[نهاية النص]