هيئة الإنترنت للأسماء والأرقام المخصصة

لجنة ابتكار تكنولوجيا المعرف - مسودة التقرير

21 فبراير 2014

جدول المحتويات

1. مقدمة 3
2. إستراتيجية اللجنة 4
3. خريطة الطريق 5
4. المسائل التشغيلية 7
   4.1. تقوية الجذر 7
   4.2. الاستنساخ 7
   4.3. السيطرة على المنطقة المشتركة 8
   4.4. عمليات السجل/ المسجلين 9
   4.5. ماهي البيانات التي ينبغي على ICANN نشرها؟ 9
      4.5.1. مقاييس ICANN 9
      4.5.2. أعياد ميلاد النطاقات وأنشطتها ومجالات سلطتها 9
      4.5.3. مثال LISP 9
   4.6. التضارب 10
5. أساسيات بروتوكول DNS 10
   5.1. المبادىء العامة 11
   5.2. نموذج البيانات 11
   5.3. التوزيع 11
   5.4. واجهة برنامج التطبيق (API) 11
   5.5. بروتوكول الاستعلام 12
6. الملاحظات والتوصيات 13
7. المراجع 14
8. معجم المصطلحات 15
9. المساهمات من أعضاء اللجنة 17
   9.1. مساهمة جيمس سينغ 17
   9.2. قرار DNS وسلوك تطبيقات قائمة البحث- جيف هاستون 18
   9.3. ملاحظات حول مساهمة الاتساق والانحراف- جيف هاستون 20
   9.4. مساهمة من بول فيكسي 21
10. الملاحق 23
   10.1. مواد LISP 24
   10.2. مواد API هوفمان 24

1. مقدمة

لقد قامت هيئة الإنترنت للأسماء والأرقام المخصصة (ICANN) بتوظيف لجنة ابتكار تكنولوجيا المعرف (ITI) لتحقيق الأهداف التالية:

1. وضع خريطة طريق تكنولوجية لمعرفات نظام أسماء النطاقات (DNS) ومعرفات أخرى
2. وضع توصيات الممارسات المثلى وأنظمة مرجعية
3. توفير الإرشاد التكنولوجي لعمليات ICANN وأمنها وسياستها ووظائفها التقنية
4. المشاركة مع مجتمع ICANN والعامة في المسائل التقنية

تم اختيار اللجنة أثناء شهري سبتمبر وأكتوبر 2013، مع بول موكابيتريس رئيساً لها. عمل جميع الأعضاء بصفتهم أفراداً، مع مناصبهم لأغراض التعريف فقط:

- جاري آركو- رئيس قوة مهمات هندسة الإنترنت (IETF)
- ريك بويفي- مركز IBM توماس ج. واطسون
- آن ماري إيكلوند لويندر- مديرة الحماية، مؤسسة بنية الإنترنت التحتية
- جيف هاستون- العالم الرئيسي، مركز معلومات شبكة باسيفيك آسيا
- جيمس سونغ- المدير التنفيذي، Zodiac القابضة
- بول فيكسي- المدير التنفيذي، Farsight للأمن
- ليكسيا زانغ- الرئيسة الرمزية لعلوم الكمبيوتر، جامعة كاليفورنيا في لوس أنجلوس

تم عقد اجتماعات شخصية في اجتماع IETF فانكوفر (نوفمبر 2013) واجتماع ICANN في بيونيس آيريس (نوفمبر 2013) ومكاتب ICANN في لوس أنجلوس (يناير 2014). كان اجتماع بيونيس آيريس مفتوحاً أمام العامة، كما تم تقديم ملخص عن أنشطة اللجنة عن طريق ندوتين إلكترونيتين في يناير 2014. النقاشات الإلكترونية عن طريق البريد الإلكتروني وما إلى ذلك دعمت تلك الاجتماعات. سيتوفر التقرير لإبداء التعليقات العامة في فبراير 2014، وسيتم إنهاؤه بعد اجتماع IETF في لندن في شهر مارس.

يود الرئيس شكر اللجنة على جميع آرائهم وأفكارهم، كما يشكر ICANN على دعم اللجنة. كما يتوجه بالشكر إلى إليس غيريتش وآليس جينسين من ICANN لمساهماتهما بالأفكار ودعم جميع أعمال اللجنة.

2. إستراتيجية اللجنة

إن اسم اللجنة ليس مصادفة. لقد توسع النطاق لما هو أبعد من DNS بحد ذاته إقراراً بالأهمية المتزايدة للمعرفات من جميع الأنواع في الإنترنت، وكذلك دور ICANN في إدارة المعرفات الأخرى. تشمل القائمة الجزئية لحافظة ICANN الحالية مايلي:

- أسماء النطاقات
- أرقام النظام المستقل
- عناوين إنترنت IPv4
- عناوين إنترنت IPv6
- عناوين البث المتعدد
- أرقام المنافذ
- أرقام البروتوكول
- سجل معرف المورد الموحد (URI)
- قاعدة معلومات الإدارة (MIB)
- قاعدة بيانات المناطق الزمنية

ولكن، بشكل يتوازى مع هذا التوسع، تم ضغط الإطار الزمني للجنة من عام واحد بالأصل إلى حوالي ستة أشهر. وأدى هذا إلى التركيز على DNS بشكل أكثر من المأمول.

للتعويض عن ذلك، تبنت اللجنة المبادىء التالية:

- محاولة توثيق جميع الأفكار قيد النظر، ولكن التركيز على قلة منها
- البحث عن ميول قوى معينة (مثل توسعة الإنترنت، الميول في هندسة المعالج)
- البحث عن الاحتياجات "الجوهرية"
- تجنب التركيز على "المجالات التي نوقشت كثيراً" (مثل نشر DNSSEC، الإستراتيجيات الحالية للتضارب) والبحث عن أفكار مبتكرة

إن الغرض الأساسي للجنة هو إثراء عملية تخطيط ICANN الإستراتيجي. رغمأن اللجنة نظرت بأفكار كانت قريبة من الاحتياجات التشغيلية لـ ICANN، فإنها لم تحصر نفسها بأفكار يمكن تنفيذها من قبل ICANN بحد ذاتها. سيقع تنفيذ العديد من الأفكار التي تمت مناقشتها هنا بطبيعة الحال على عاتق IETF أو غيرها. تثير بضعة أفكار مسائل متعلقة بالسياسة لم نناقشها بقدر ما أشرنا إليها فحسب.

مؤخراً، نظراً للقدر الغامر من الأنشطة في مساحة المعرفات، بالكاد استطاعت اللجنة مناقشة عينة عن هذه المساحة. ينبغي ألا يفترض القارىء أننا كنا نعرف جميع الأنشطة الجارية، أو أن الأفكار التي لم تتم مناقشتها هنا ذات أهمية أقل.

3. خريطة الطريق

إن المعرفات هي مجال بالغ الأهمية في مجتمع الإنترنت. على المدى القصير، ستصبح نطاقات المستوى الأعلى (TLDs) الجديدة عاملة. سيصبح حسابك على الفيسبوك اعتماد تسجيل الدخول الوحيد لك على الإنترنت- وكذلك حساب غوغيل. على المدى البعيد، ثمة عدة مشاريع مختلفة لمجتمع الأبحاث ومن بينها الشبكات المحورية للمحتويات (CCN) والشبكات المحورية للمعلومات (ICN) وشبكات البيانات المسمية (NDN) والعديد من المتباينات الأخرى. رغم عدم اتفاقهم على اسم للمجال، فإنهم يتفقون جميعاً على أنه ينبغي تحديد المحتويات بالاسم، وليس الموقع، وبأن الإخفاء يجب أن يكون انتهازياً. أصرت مقترحات أخرى على أن الأسماء المسطحة هي الموجة المستقبلية، وينبغي أن تكون الأسماء ذاتية الاعتماد هي أساس أي نظام جديد.

إن المعرفات هي محورية لأية شبكة من ناحية المكونات المعرفة بشكل فردي للشبكة إلى جميع المكونات الأخرى للشبكة. بالإضافة إلى ذلك، فإن الشبكات الحديثة ليست نطاقاً فردياً متجانساً، ولكن يتم اعتبارها على أنها مزيج من عدد من التقنيات، وثمة متطلب للتوجيه بين مجالات الهوية. يتم القيام بوظيفة التوجيه هذه بعدة طرق. ضمن سياق الإنترنت، أحد أكثر مجالات الهوية المرئية هو مجال اسم النطاق، والذي يقوم بهيكلة مساحة الاسم بشكل هرمي. ترتبط مع مساحة الاسم وظيفة التوجيه التي يمكنها التوجيه من أسماء النطاقات إلى معرفات أخرى (مثل عناوين بروتوكول الإنترنت). عندما ننظر في أمر خريطة طريق للمعرفات، ينبغي أن ندرك الفرق بين مجال المعرفات ووظيفة التوجيه، والنظر في خريطة الطريق لكل منهما.

في الإنترنت الحالية، حددت اللجنة عدة عوامل ستميل إلى توسعة استخدام DNS، بالإضافة إلى عوامل أخرى ستعمل على اجتذابه. ليست جميع هذه العوامل تقنية، ويبدو الصراع اصطفافاً طبيعياً أكثر مما هو مبني على التأنق أو أية فضيلة أخرى.

عوامل التوسعة الحالية

- يتمتع DNS بميزة الإرث من ناحية أنه تم تنفيذه في كل جهاز يلمس الإنترنت. مجرد النمو بقاعدته القائمة سيوسع نموه. على سبيل المثال، البرنامج الذي يود عبور الجدران النارية والتخزين في أنحاء الإنترنت سيجد DNS كقاعدة قائمة.
- ستحاول TLDs الجديدة استغلال ماركاتها. رغم أن الكثير من الشكوك تحوم في المجتمع التقني، ستصارع أكثر من ألف ماركة جديدة للازدهار، ومن المرجح حدوث ابتكار والعديد من المفاجآت.
- إن القدرات الجديدة المنبثقة، مثل القدرات الأمنية لامتدادات أمن نظام أسماء النطاقات (DDNSSEC) أو التحقق من صحة الهيئات المسماة بحسب DNS (DANE)، قد تحفز المزيد من الاستخدام.
- قد توسع البيانات الجديدة في DNS من استخدامها، وخاصة عند دمجها مع DNSSEC لضمان التحقق من الصحة. دافع أحد أعضاء اللجنة عن نشر "عيد ميلاد" و"نشاط" النطاقات كمعلومات سمعة رئيسية. استخدمت مقترحات أخرى DNS كسجل لكتل العناوين وما إلى ذلك. قيدت ICANN استخدام بعض الملصقات في أسماء النطاقات، وقد يكون سجل بالوقت الفعلي كهذا مناسباً، وخاصةً عندما تكون المواصفات الورقية بأحرف أبجدية متعددة.

عوامل التقلص الحالية

- إن DNS هومعيار موروث، ولكن هذا يشكل عائقاً أيضاً من ناحية أن منطق DNS المتجسد في نقاط ولوج WIFI وموديمات خط المشترك الرقمي (DSL) والكيبل والجدران النارية والأجهزة التوجيه وقاعدة البرمجيات للإنترنت غالباً ما تحد من نطاق الاستخدام وتقيد الابتكار. غالباً ما يكون التنفيذ أقل من مكتمل، أو محدّث أو متوافق مع المعايير. لقد أعاقت هذه المسائل من تنفيذ DNSSEC وجعل تنفيذ أية مميزات أو أنواع بيانات DNS مثيرة للمشكلات. سيؤدي هذا إلى وضع ممارسات مثل اقتصار جميع الاستخدام على سجلات العنوان والنص (TXT). هذا التحجر لا يقتصر على DNS.
- ثمة اهتمام تجاري بالسيطرة على ("امتلاك") نافذة البحث و/ أو مساحة المعرف. الاهتمام هنا هو بمعرفة نية المستخدم في الشكل الحر وإبقائها مخفية عن الإنترنت المفتوح. لقد لاحظنا ميل الأجهزة ذات الرموز الصعبة إلى خدمة DNS معينة، بالإضافة إلى الامتدادات مسجلة الملكية، كطريق إلى البلقنة.
- يفضل المستخدم واجهة أقوى. بدلاً من إدخال أسماء DNS، غالباً ما يوظف المستخدمون والبرامج البحث وآليات أخرى للوصول إلى معلومات معينة. على سبيل المثال، فإن شريط محدد مواقع المورد الموحد (URL) هو أداة بحث واسعة الاستخدام اليوم. واجهة مستخدم اليوم هي الجهاز الخلوي، والذي لا يفضل الطباعة. يؤدي التعرف على الصوت وأنواع أخرى

من الذكاء الاصطناعي (AI) في شريط المتصفح إلى انعدام توافق بين البائعين المختلفين. كمثال على ذلك، راقبت تجربة أجراها جيف هستون (شاهد المساهمة) عمليات البحث التي أثارها "Geoff.Huston" في عدة متصفحات، ولاحظت عدم اتساق تقريباً بين جميع البائعين. يمكن التساهل مع انعدام الاتساق هذا في بحث المتصفح حيث يكون متوقعاً من المستخدم مراجعة النتائج، ولكن يمكن أن يكون خطيراً في ملفات التهيئة في الأنظمة- إحدى المخاوف تتعلق بالتضارب.

كان رأي اللجنة أنه رغم أن استخدام DNS يضعف تدريجياً من واجهة المستخدم، من الأرجح أن يظل أداة بنية تحتية. أحد التشبيهات هو أن DNS ليس عبارة عن الورق بمواجهة هجمات الكتب الإلكتروني، بل بالأحرى مجموعة تعليمات كمبيوتر يمكن الولوج إليها عن طريق لغات مستوى أعلى.

اختلفت الآراء حول ما إذا كان من الممكن أو من الحكمة السعي نحو نهضة DNS أو إعادة تركيبه. وقد تمت مناقشة التقنية في قسم "أساسيات DNS" من هذا التقرير. ثمة سؤال يتعلق بالسياسة حول ما إذا كان ينبغي على ICANN محاولة الحفاظ على نظام DNS وتوسعته. إذا صح ذلك، كيف سيحصل المرء على هندسة متسقة بناءً على الآراء المتنوعة لدائرة ICANN وIETF (حيث يفترض أن يتم إنجاز العمل) والأطراف الأخرى للإنترنت؟

<u>المدى الطويل</u>

إحدى مجموعات الأفكار على المدى الطويل هي نموذج شبكات البيانات المسمية. أفكاره الرئيسية هي الولوج إلى المحتويات بحسب الاسم والتحقق من الصحة الرقمي في كل مكان والتخزين الانتهازي ومخطط متدفق حيث تتبع طلبات وردود المحتويات نفس الدرب. يتم التعبير عن نموذج توجيه الاستعلامات أحياناً على أنها مجرد استخدام لهرمية الاسم لأطول قرارات توجيه مطابقة سابقة يجدها المتشككون غير قابلة للقياس. على أي حال، تم تنفيذ أجهزة بحث للبرمجيات والمعدات والعديد من الشبكات. إن التطبيقات الأوضح هي توزيع المحتويات، ولكن يدعي المدافعون أن النموذج هو مناسب للسيطرة على العملية والشبكات الآلية وما إلى ذلك.

ضمن هذا المعنى، كان DNS هو الأول من بدائل الصفحة القذرة لتنقية ICN، تماماً مثل المناهج الأحدث [فايز بقش 2013] التي تحاول الحفاظ على الأجزاء الأهم من نموذج ICN. الأهمية هنا هي بعين الناظر.

يستعيد DNS البيانات بحسب الاسم. ولايحاول التوجيه بالاسم، ويستخدم بدلاً من ذلك طبقة عناوين الإنترنت، ويصلح هذا المخطط ما يعتبره البعض مشكلة قياس مركزية في ICN. يشتهر DNS بشكل سيىء بأنه مركبة لتوجيه الفيديو [كامينسكي 2004] ويحظر توجيه الولوج عن طريق استعلامات DNS التي يتم القيام بها قبل التحقق من الصحة من قبل بعض نقاط ولوج WIFI. (بحث "توجيه DNS" على غوغيل يؤدي إلى 1,620,000 نتيجة).

ICN ذات مطابقة سابقة أطول وباحثين يحق لهم السماح بنقل الوسائط، وهي تسهيلات تم توقعها في قسم الاستعلام من مواصفات بروتوكول DNS الأصلي، ولكن لم يتم تطويرها.

على أي حال، على افتراض أن بوسع المرء جعل باقات DNS أكبر وإضافة بعض حقول الاستعلام الإضافية، يمكن استنساخ خدمات المحتويات في DNS. قد تكون مطابقة ICN للطلبات والردود المتحقق من صحتها هي أفضل وسيلة لتجنب هجمات تضخيم DNS.

بالختام، يمكن للمرء تصور مخطط استبدال NDN لـ DNS، وعلى الأرجح سيبدأ كمجوعة فرعية من تسهيلات DNS في انتقال سيستغرق اكتماله سنوات أو عقود. أية محاولة لتعزيز هندسة DNS ينبغي أن تستعين بحرية من NDN.

ICN ليس بأي شكل من الأشكال النموذج الوحيد للمستقبل، ولكنه الأكثر تطوراً. إننا نعتقد أنه من المفيد دائماً محاولة استخراج المبادىء الرئيسية، ثم دراسة التركيب. [غودسي 2011] هو مثال جيد على طريقة نقله ثالوث الاسم والهوية بالعالم الحقيقي والبنية التحتية الرئيسية العامة (PKI).

مؤخراً، ظهر على السطح تركيز على توزيع السيطرة [نيويوركر 2014] والخصوصية، ونظام نيمكوين هو المثال الأوضح عليها. إن PKI القائمة تمثل مورداً على المراقبة واسعة المدى، وبالتالي، تشكل مشكلة على الخصوصية. قد يكون مزيج من العناصر ذاتية الاعتماد وPKI اختيارية أو ربما PKIs متوازية وأنظمة نظير إلى نظير (P2P) هو الحل.

4. المسائل التشغيلية

تنشأ العديد من المسائل في عمليات ICANN اليومية. وتدور معظمها حول الجذر.

4.1. تقوية الجذر

نظراً للأهمية المحورية للبنية التحتية للجذر، تم تقديم عدة اقتراحات خارجية بأن تنظر اللجنة في تكنولوجيا الاحتساب الموثوقة. وجدت اللجنة أنه قد يكون ثمة جدوى من هذا النوع من التكنولوجيت في الأنظمة المستخدمة لتحرير وتوقيع الجذر، ولكنها وجدت أن النظر بتحسين توزيع البيانات الموقعة على معدات المجتمع سيكون أولوية أفضل للجنة. أثارت اكتشافات سنودين بعض المخاوف الأمنية حول المعدات لم يتم النظر بها في تصميم الأنظمة الحالية، مثل عدوى BIOS وبرامج التجسس على القرص الصلب وما إلى ذلك [سبايغل 2014].

4.2. الاستنساخ

لطالما امتلك DNS آليتين إضافيتين لتوزيع البيانات: الاستنساخ المخطط له مسبقاً للمناطق والاستعلامات عند الطلب. من منظور القطعة الفردية من بيانات DNS، يبدأ سجل المورد (RR) على أنه المورد المثالي كجزء من المنطقة وينتقل مع تلك المنطقة في انتقال واحد أو أكثر، ثم يكمل رحلته إلى وجهته النهائية عند سحبه عن طريق الاستعلام.

على سبيل المثال، تستخرج ICANN منطقة الجذر بالشراكة مع Verisign ووزارة التجارة الأمريكية، ثم يتم توزيعها على جميع مخادم الجذر عن طريق انتقالات المنطقة. بالتالي، يمكن القيام بذلك التوزيع، مثل توزيع أية منطقة أخرى في DNS، عن طريق أية آلية: شرائط مغناطيسية وتسليم فيديرال إكسبريس (FEDEX)، أو انتقال الملفات عن طريق بروتوكول نقل الملفات (FTP) أو Rsynch، أو بشكل مثالي أكثر عن طريق نقل الجذر التدريجي الذي يرسل التغييرات من نسخة سابقة بدلاً من المنطقة بأكملها. يمكن إما نشر النسخ عن طريق إشعار DNS أوسحبها عن طريق إستراتيجية اقتراع تنظر بالتغييرات. يمكن تأمين حماية انتقالات المنطقة عن طريق توقيع معاملة DNS (TSIG) و/ أو أي عدد من بروتوكولات النقل، مثل أمن بروتوكول الإنترنت (IPSEC) وأمن بروتوكول نقل النص الفائق (HTTPS) وما إلى ذلك. ثمة مئات حالات مخادم الجذر مع نسخ عن منطقة الجذر.

عندما يرغب المستخدمون بالولوج إلى بيانات في منطقة الجذر، سيرسلون استعلامات إلى الجذر. يتم توجيه الاستعلامات بواسطة آليتين: أولهما هي عنوان وجهة بروتوكول الإنترنت في معرفات الاستعلام تحدد مجموعة من مخادم الجذر التي تشترك بعنوان أنيكاست شائع، وثانيهما هي أن يقرر نظام التوجيه المخدم في مجموعة أنيكاست الذي سيستلم الاستعلام. هذا المخطط هو نتيجة لتطور بدأ مع 3 مخادم جذر ذات عناوين بث موحدة، ثم تمت توسعتها إلى 13 منظمة مخدم جذر مع تجمعات تتشارك بالحمولة، ثم المخطط الحالي (مع العديد من الخطوات الأصغر بينها). بكلام مبسط أكثر، "13 مخدم جذر" هي بالواقع "13 منظمة مخدم جذر" تسلم في النهاية المنطقة إلى مئات أو آلاف المخادم الفردية[1]. سبب وجود 13 منظمة مخدم جذر فقط، واستخدام أنيكاست، هو أن فعل ذلك أسهل من تخفيف حدود حجم باقات بروتوكول حزمة معلومات المستخدم (UDP) لـ DNS. كما أن ثمة عدة مشكلات حجم مرتبطة بإضافة عناوين IPv6. على المسار من مخدم الجذر إلى المستخدم، يمكن توفير الأمن عن طريق DNSSEC بشكل اختياري.

على مدار السنوات، تعرضت مخادم الجذر للهجمات، ومعظمها على تباين رفض الخدمة المتوزع (DDOS). لكي ينجح مثل هذا الهجوم ضد مستخدم معين، يجب أن يعطل الاستعلامات إلى جميع عناوين أنيكاست لمنظمات مخدم الجذر الـ13 المختلفة. إن تعطيل مجموعة فرعية سيبطيء الأداء بينما يتعلم الطالب أية مخادم جذر عليه تجنبها. يمكن أن يكون التعطيل إما بإيقاف المخدم أو مسار الشبكة إلى المخدمة، بحمل زائد بالعادة. لذا، على سبيل المثال، في مثل هذه الهجمات، ظن المستخدمون في كاليفورنيا أن مخدم الجذر في ستوكهولم قد تعطل، وفي ستوكهولم لاحظ المستخدمون العكس. كانرد منظمات مخدم الجذر على التهديد الأخير من منظمة متسللي الإنترنت المجهولة هو نشر المزيد من الحزمة العريضة والمخادم والضوضاء.

[1] واليوم، تشغل نفس الهيئة، وهي Verisign، اثنتان من منظمات مخدم الجذر

وبالطبع، لا داعي لتوجيه الهجمة نحو تجمع مخدم الجذر، بل يمكن توجيهها ضد وصلة (وصلات) المستخدم بالإنترنت. رغم أن أضرارها محدودة أكثر، فإن العلاقة المتبادلة للقوى بين الهجوم على الشبكة الآلية وشركة واحدة غالباً ما تكون لصالح المهاجم حتى للشركات الأكبر.

يمارس بعض أعضاء اللجنة تقديم توصية إلى الشركات بتوزيع نسخة من الجذر داخلياً، **وأية مناطق حيوية أخرى**، حتى يستمر التشغيل العادي في DNS على الأقل أثناء الهجمة. تسهل ICANN على أية منظمة الحصول على نسخة من مخدم الجذر، ومع المزيد من العمل لتصبح مثال مخدم جذر في منظمة مخدم جذر ICANN. كما أنه سيكون من الجيد أن تكون الشركة مكتفية ذاتياً فيما يتعلق بـ DNS، وعدم تعرضها للتهديد بسبب انعدام الولوج إلى المخادم الخارجية، أو إجراءات من سجل أو مسجل أو مخدم جذر أو ما إلى ذلك، سواء بالخطأ أو بشكل مقصود.

نظراً لـ DNSSEC، لدينا وسيلة لتوزيع منطقة يمكن التحقق منها باستخدام التواقيع الرقمية المغروسة. إننا نعتقد أنه يمكن توسعة المبدأ أكثر، عن طريق حماية التفويض والبيانات المعلقة على سبيل المثال. قد يكون من الممكن أيضاً التخلص من أو تخفيف منظمة مخدم الجذر وبيانات العنوان. إحدى المخططات، المبينة بالتفصيل في مساهمة بول فيكسي، هي متضمنة في قسم المساهمات من هذا التقرير.

وثمة جوانب سياسية مهمة أيضاً. ثمة 13 منظمة مخدم جذر، وتشعر العديد من الدول أنها معزولة، حتى لو حظيت بالعدد الذي ترغب بتركيبه من حالات مخدم جذر ICANN في بلادهم. (ناهيك عن ذكر العديد من منظمات مخدم الجذر الأخرى المستعدة لتوسعة تجمعات أنيكاست الخاصة بها). إذن فلنترك مناقشة هذه المسألة.

ينبغي التنويه أنه ليس ثمة حاجة تقنية لاستبدال نظام مخدم الجذر الحالي لأولئك الذين يفضلونه، لنجعل الاستنساخ أسهل للجذر، وكذلك نحدد قدوة للمناطق الأخرى.

4.3. السيطرة على المنطقة المشتركة

في قسم سابق، ناقشنا الآراء السياسية التي تجعل الدول ترغب بامتلاك منظمة مخدم جذر. قد تكون هذه المخاوف صحيحة أو غير صحيحة، ولكن ثمة شك بأن تشغيل الجذر الحالي مقره في الولايات المتحدة ويخضع لصلاحيتها القضائية.

بعبارة بسيطة، يتم تحديث الجذر بهذا الترتيب:

- تتلقى ICANN طلبات التحديث من TLDs، وتدقق بها بحثاً عن أخطاء
- ترسل ICANN التغييرات إلى وزارة التجارة
- ترسل ICANN التغييرات المعتمدة إلى Verisign
- تستخرج Verisign جذر موقع وتوزعه

هل ثمة طريقة تقنية للتفكير بمشاركة السيطرة على الجذر؟ لقد تقدمت بعض النظريات. إحدى المدارس الفكرية هي أن البيانات ينبغي أن تحمل س من التواقيع المتعددة. ثم س/ ص، التواقيع هي متطلبة للتحقق من صحة البيانات. وبالطبع، ثمة حجج حول س وص، وما إذا كان التشفير المختلف هو ضروري/ مرغوب به.

لا نهدف هنا إلى الدفاع عن نظام معين، ولكننا نشعر أن التصميم الجيد قد يسمح للعملية السياسية باتخاذ قرار حول كيفية البدء بمشاركة السيطرة. رؤيتنا هي إنشاء صندوق أدوات للسيطرة المشتركة على المنطقة، وليس للجذر فقط، بل لمشكلات تنسيق المنطقة الأخرى. إننا ننوه أن مجموعة عمل عمليات DNS (أو DNSOPS) في IETF تقدم بمقترحين لتنسيق معلومات توقيع DNSSEC، ولكننا نتساءل ما إذا كان من الأفضل إنشاء مرافق عامة بدلاً من حل لمشكلة هذه النقطة. تنسيق العناوين المرسلة والمعكوسة قد يكون تطبيقاً آخر.

ما هو المتطلب إذن؟ إننا نخمن بأن النموذج المناسب الذي تتشارك به جميع الأطراف السيطرة يتمتع بمجموعة من القدرات:

- نظام لمباشرة المنطقة المشتركة يتألف من المنطقة نفسها والقوانين ويوميات فردية لكل من المشاركين لكي ينشروا طلباتهم وإجراءاتهم
- كل نوع من الطلبات هو مرئي لجميع المشاركين الآخرين الذين يمكنهم اعتمادها أو عدم اعتمادها أو توقيتها
- قوانين تحدد ما يحدث للطلب
  - أحد أنواع القوانين هو تصويت يحدد شروط نجاح الطلب. قد يشمل هذا تأخيراً لجميع الأطراف لكي تحظى بوقت للنظر بالطلب.
    - بالنسبة إلى ccTLDs، قوانين WSIS ستملي 1 من س، حتى يتمكن كل نطاق مستوى أعلى لرمز الدولة (ccTLD) من تغيير بياناته من طرف واحد.
    - يمكن لنطاقات أخرى استخدام أغلبية بسيطة
  - قد تكون التأخيرات المحددة مهمة حتى يتمكن الآخرون من الإشارة إلى المسائل التشغيلية والسماح للطالبين بإعادة النظر
  - قد تنطبق ظروف مختلفة على العمليات المختلفة، مثل إنشاء الجديد مقابل التحرير وما إلى ذلك.

ثم يمكن لكل مشارك عندها القيام بخوارزمية معيارية لاستخراج الحالة المتسقة. قد يبدو هذا خيالاً، ولكن الخوارزميات البيزنطية مثل بيتكوين [آندريسين 2014] ونيمكوين تثبت أن مثل هذه الأنظمة هي ممكنة اليوم.

(يرجى الملاحظة أننا لا نقترح القوانين، بل مجرد نظام توزيع لتنفيذ أية قوانين يرغب بها المجتمع).

4.4. عمليات السجل/ المسجلين

جادل بعض أعضاء اللجنة بأنه ينبغي أن توفر عمليات ICANN ضمانات مستوى خدمة، ولكن لم يكن من رأي اللجنة أنها مسألة يمكن ان تحرز تقدماً.

4.5. ماهي البيانات التي ينبغي على ICANN نشرها؟

4.5.1. مقاييس ICANN

تدير ICANN العديد من مجموعات المقاييس كجزء من وظائف هيئة أرقام الإنترنت المُخصصة (IANA)، بالإضافة إلى عملية TLD الجديدة، وغير ذلك، مثل الملصقات المعكوسة في عدة لغات. ينبغي توفير هذا كله عبر الإنترنت، ربما في DNS، وبشكل آمن بالتأكيد، حتى يتم استخدامها مباشرة من قبل أي شخص في مجتمع الإنترنت.

4.5.2. أعياد ميلاد النطاقات وأنشطتها ومجالات سلطتها

إن سمعة DNS هي أداة حماية قيّمة. قد يكون تاريخ إنشاء نطاق ما هو قطعة المعلومات الفردية الأكثر دلالة. قطعة أخرى هي معدل تحديث النطاق لأسماء وعناوين المخدم. النطاقات الجديدة ونشاط التحديث المرتفع هي مثيرة للشكوك. سيكون من المرغوب توفير هذه المعلومات في الوقت الفعلي.

تمت مناقشة معلومات مجالات السلطة بشكل مشابه، ولكن ستناقشها IETF في اجتماعها التالي في لندن في شهر مارس 2014.

4.5.3. مثال LISP

في وقت مبكر، تم الطلب من اللجنة النظر بجعل ICANN تدعم خدمة جذر فائق لبروتوكول فصل محدد المواقع/ المحدد (LISP) [RFC 6830]. كما شرح لنا دينور فاريناتشي وآخرين، ستشغل ICANN مخادم LISP كخدمة تجريبية لإحالة الطلبات إلى مخادم

LISP الحالية التي لا توفر اتصالاً عالمياً حالياً. لقد حددنا موارد لأربعةمخادم، ولكن لم يبدأ المشروع بسبب بعض المسائل غير المحلولة:

- ما هو نطاق (المدة وما إلى ذلك) التجربة؟ ما هي معايير النجاح؟
- ما هي البرمجيات التي ستستخدم ومن سيدعمها؟ كان يتوفر بديلين مسجلي الملكية.
- من سيتمتع بالسيطرة التشغيلية وعلى السياسة؟
- هل ينبغي على ICANN فعل ذلك أم سجلات الإنترنت الإقليمية (RIRs)؟
- هل سيتغير الرد إذا لم تكن عناوين بروتوكول الإنترنت مشمولة؟

مواد LISP هي مرفقة كملحق. لم يتم اتخاذ أي إجراء في هذه التجربة.

شعر بعض أعضاء اللجنة أن "LISP هي مجرد مثال واحد على طبقة عامةأكثر لتقنيات توجيه النقل، وبالتالي، لم تمثل أيةمهمات إدارة معرف مبتكرة تقع خارج ممارسات إدارة المعرف التشغيلي الحالي، وبالتالي، فإنحال تطلب هذا الشكب بالذات من التوجيه إلى عناية خاصة ودعم خاص من ICANN لم تكن مدعومة بأدلة كافية".

ينبغي على ICANN توقع أن الأسئلة التقنية والمتعلقة بالسياسة حول المعرفات الجديدة ستظهر من جديد، والتخطيط وفقاً لذلك.

4.6. التضارب

العديد من أعضاء اللجنة مطلعين جيداً على مسألة تضارب DNS، ورغم الحوار المطول حول هذه المسألة، لم يتم التوصل إلى توجيهات جوهرية جديدة. شعرت اللجنة بأن وضع النموذج الأولي من النظام المبين في [ICANN 2013] هو أمر موصى به.

5. أساسيات بروتوكول DNS

هل يمكننا تصور مراجعة أساسية أو ترقية أو نهضة في DNS؟ يعتقد العديدون، ومن بينهم بعض أعضاء اللجنة، أن القاعدة المثبتة هي شديدة المقاومة، أو العملية متعطلة، أو البدء من جديد هو فكرة جيدة.

بشكل مفاجيء، أجمعت اللجنة على الاعتقاد بأن بذل الجهود لتشخيص هذه المسائل والبحث عن حلول تستحق العناء، ولو حتى لإنهاء هذه المسألة على الأقل. في هذا القسم، سنحدد المسائل التي ينبغي دراستها إذا كان ينبغي التعهد ببذل جهود أوسع.

لقد حقق تاريخ الابتكار في DNS النجاح والفشل. أحد الدروس الرئيسية هو أنه لا يتم تبني التكنولوجيا بشكل واسع إلا إذا وفرت ميزة معينة. يلتزم الإداريون الحرص بالحفاظ على اتصال مناطقهم مع DNS العالمي وتحديث سجلات A وMX، وإلا لن يحصلوا على حركة بريد أو ويب. ولكن من بين حوالي 60 نوع سجل تم تحديدها، أقل من 10 تشهد استخداماً واسعاً.

واجهت جهود إنشاء برنامج صعوبات مماثلة.

اقترحت أول مجموعة من DNS RFCs وسيلة لتوجيه البريد إلى صناديق بريد معينة، ولكن لم يتم تنفيذها قط. المخطط الثاني، وهو MX RR، حل مشكلة توفير مخادم بريد متكررة، بالإضافة إلى توفير توجيه البريد عن طريق الحدود التنظيمية- وهي أساس توجيه البريد اليوم. تم تبني قواعد بيانات مضاد البريد الدعائي بشكل واسع من دون تحديد معايير. أدت جهود المعايير المتضاربة للتحقق من صحة البريد إلى تنفيذين اثنين باستخدام TXT RRs، وجدال حول ما إذا كان وضع معايير أنواع جديدة سيكون مفيداً.

كما أن جهود توجيه الرقم E.164 (ENUM) لتحديد معايير الهواتف وتوجيه الوسائط الاخرى باستخدام DNS حققت نجاحاً محدوداً. ورغم اعتبار تكنولوجيا مؤشر هيئة الأسماء (NAPTR) على أنها ابتكار حقيقي، تجاهل مصممو ENUM الحاجة إلى توجيه المعلومات الأخرى غير رقم هاتف الوجهة، وفضل مصنّعو المعدات الحفاظ على القيمة في أنظمتهم مسجلة الملكية.

5.1 المبادىء العامة

ينبغي أن يتمتع أي تصميم جديد بمايلي:

- إزالة تحديدات الحجم- من الأرجح أن وحدة نقل الحد الأقصى بـ 576 بايت (MTU) قد أعاقت DNS أكثر من أي عامل فردي آخر، DNSSEC لا يتناسب وباستثناء آلية توسعة DNS (EDNS0)، فإن العديد من المعدات والبرمجيات لا تنقل باقات كبيرة.
- الحفاظ على قابلية الاتصال
- محاولة رعاية التطبيقات المتسقة- إذا لم تتبع التطبيقات المختلفة المواصفات، فسيتقيد المستخدم عندها بالتضارب المشترك القائم أياً كان
- السماح بالتوسع المستقبلي
- توفير حوافز للتبني

5.2 نموذج البيانات

تصورت DNS RFCs مساحات الاسم المتوازية "لطبقات" مختلفة من المعلومات، وأنواع البيانات الجديدة التي تتألف من مكونات بسيطة. لم يتم استكشاف فكرة الطبقة. تم تحديد أنواع بيانات جديدة، ولكن مؤخراً، يجادل العديدون بأن استخدام سجل TXT العام يعني أن تنقل سلاسل نصية اعتباطية البيانات، إلى جانب مستوى آخر من الملصقات كوكيل عن نوع RR.

سنجادل بأنه ينبغي على DNS تعريف أنواع RR الخاصة بها والتنسيقات في البيانات حول البيانات المنقولة في DNS، أو ينبغي علينا رسملة الملصقات التابعة على أنها آخر نوع من البيانات وتوسعة الاستعلام للسماح بمطابقة مرنة أكثر.

في النهاية، علينا استكشاف البيانات الموقعة ذاتياً التي يمكن أن تبقى مستقلة في اسم النطاق.

5.3 التوزيع

يتم تنفيذ هيكل المنطقة للبيانات والتخزين بحسب سجل المورد "بتحسينات" غير متساوية إلحد ما على معيار الوقت للاستمرار (TTL)، والاستدعاء المسبق للمعلومات منتهية الصلاحية. قد يستحق العناء النظر بوسائل جديدة لجمع البيانات مع أرقام تسلسلية قد تجدد مجموعات البيانات المخزنة من دون نقل البيانات فعلياً.

كما نعتقد أنه يمكن تحسين الأمن عن طريق الاستنساخ المتكرر أكثر للمناطق (الأصغر). لا تحتاج هذه البيانات إلى الحماية من DNSSEC، وبالتالي، يمكن تحسين الأمن في المناطق التي لا يتم تنفيذ DNSSEC بها.

5.4 واجهة برنامج التطبيق (API)

ثمة شكلين اثنين لـ DNS API: واجهة المستخدم والأسماء على مستوى API. في كلتا الحالتين، سنستفيد من تركيب معياري يسمح باسم نطاق مؤهل بالكامل (FQDN) صريح. ستتم خدمة مجتمع المستخدمين بشكل أفضل عن طريق مجموعة متسقة من سياسات البحث على نطاق UIs، ولكن ليس من الواضح إن كان ثمة وسيلة لجعل البائعين يقومون بذلك.

خضعت API البرمجة للعديد من محاولات المراجعة، ومعظمها فشلت. مؤخراً، سمعنا محاضرة من بول هوفمان حول تصميم جديد يضم واجهات غير متزامنة ودعم من DNSSEC. راجع الملحق. إننا نفهم بأنه يجري العمل الآن في مختبرات Verisign وNLnet، ولكننا لم نتمكن من الحصول على المزيد من المعلومات، رغم أننا سمعنا أن الإصدار هو وشيك.

ولكن بغض النظر عن API، ثمة سؤال مرتبط بمكان تنفيذ التحقق من DNSSEC وفلترة DNS (إن وجدت). أجمعت اللجنة على أنه ينبغي السماح بإنهاء DNSSEC تقنياً في النظام النهائي (والذي قد يكون آلة افتراضية أو كمبيوتر محمول أومخدم في بيئة المستخدموما إلى ذلك، بحسب تفضيل المستخدم) رغم حقيقة أن هذا قد يكون مستحيل بسبب جهاز التوجيه أو الجدار الناري أو القيود الموروثة الأخرى. بشكل مشابه، رغم أن فلترة DNS ليست المفضلة للجميع، ينبغي أن تكون تحت سيطرة المستخدم.

ينبغي ألا يعني شيء من هذا أن المستخدم ممنوع من التوريد الخارجي لهذه المهمات إلى ISP أو أية خدمة أخرى.

قد تنص قيود السياسة والقيود القانونية على غير ذلك.

بروتوكول الاستعلام

5.5. بروتوكول الاستعلام

ثمة نوعين من المسائل يرتبطان ببروتوكول استعلام DNS: تلك المرتبطة بنقل الاستعلامات/ الردود من طالب إلى مخدم، والنوع الثاني هو تضخيم قوة الاستعلام.

بدأن مسائل نقل UDP الأصلية مع تحديد MTU الـ 576 بايت التقليدية. كان الإصلاح الأصلي هو الرجوع إلى TCP لعمليات النقل الأكبر. الأرجح أن حجم بيانات الجذر هو أول مكان أحدثت به تحديدات MTU تأثيراً واسع النطاق أدى إلى حدود 13 مخدم جذر، ثم لاحقاًإضافة توقيعات DNSSEC الجذرية التي وسعت كثيراً من باقات الرد. تم التفكير بـ EDNS0 لحل هذه المشكلة، بالإضافة إلى أمور أخرى، وحققت بعض النجاح. ولكن ثمة تحديدات أخرى مثل حجم إطار إيثرنت 1582 أو 1280 لـ IPv6، التي تحد من UDP بشكل أساسي.

كما أن EDNS0 لا يحل مشكلة نقاط الولوج وأجهزة التوجيه والجدران النارية والمعدات الأخرى التي تحجب الولوج إلى منفذ TCP رقم 53، أو تحد من حجم الباقة، أو حتى تعترض طلبات DNS في البروكسي الشفاف، غالباً إلى درجة إعاقة الخدمة. قد تعاني مخادم تخزين الأسماء التي لا تدعم الباقات الكبيرة، وجميع أنواع بيانات DNS وEDNS0 وما إلى ذلك.وقد تكون بعض المشكلات صعبة للغاية. في أحد الأمثلة، تمر باقات DNSSEC بالعادة ولكن ليس أثناء التقلب الرئيسي لـ DNSSEC، وهي عملية صيانة اعتيادية، حيث تكون الباقات أكبر قليلاً.

إحدى المشكلات المرتبطة هي هجمات DNS DDOS، وخاصة باستخدام الانعكاس والتضخيم. في تلك الحالات، سترغب بطريقة لتحديد الحركة الشرعية من حركة الهجمات. سيحل التحقق من صحة العناوين جزءاً كبيراً من المشكلة، لـ DNSوالعديد من البروتوكولات الأخرى. تدعم اللجنة ذلك، ولكن لم يتم نشره بشكل واسع. يمكن أن يساعد تشكيل النسبة والمناهج التجريبية المتنوعة، ولكنها ليست حلاً حاسماً. تظل آليات التحقق من الصحة الحفيفة المتنوعة وستظل حلولاً محتملة.

إحدى المدارس الفكرية لحل مشكلة النقل هي وضع جميع حركة DNS في https:. يكمن المنطق وراء ذلك بأن لدى الجميع مصلحة في رؤية تدفق حركة ويب آمنة، وبالتالي، فإنه مسار مضمون (ويقول البعض إنه المسار المضمون الوحيد). والثمن هو حالة اتصال والنفقات العامة المرتبطة بها. تشمل البدائل بروتوكول معاملة جديدة أو وسيلة لاستخدام UDP، وكلاهما قد لا يعملان في أجزاء من القاعدة المثبتة. في كلتا الحالتين، ثمة مسألة ما إذا كانت معاملات DNS تستخدم شكلاً تقليدياً أو جديداً.

بغض النظر عن النقل، ينبغي توسعة بروتوكول استعلام DNS للسماح بالمزيد من الاستعلامات المرنة. وقد تشمل نوعاً ما من التحكم بالولوج إلى الملصقات الوريثة بدلاً من NSEC.

تعلمت بروتوكولات عالم الأبحاث مثل CCN من DNS ودمجت جميع هذه المميزات. المشكلة تتعلق أكثر بتحديد كيفية تحفيز ترقية للبنية التحتية القائمة مع بعض التوافق الرجعي، بدلاً من تحقيق انفراج جديد في علم البروتوكول.

6. الملاحظات والتوصيات

- سيستمر استخدام DNS في البنية التحتية بالنمو، ويواجه استخدام DNS في واجهة المستخدم (UI) تحديات من البدائل المبنية على الأبحاث وواجهات الهاتف الخلوي وما إلى ذلك.
- ينبغي على ICANN نشر المزيد من بيانات DNSSEC الموقعة للملصقات المحجوزة وما إلى ذلك.
- بالتعاون مع IETF وآخرين، تم إجراء دراسة لتحديد نظرة هندسية لـ DNS في عام 2020.
- تصميم ووضع نموذج أولي لنشر الجذر المفتوح.
- تصميم نظام تحكم بالمنطقة المشتركة للجذر.
- إجراء تماريت تصارب لاختبار سهولة التنفيذ [ICANN 2013].

7. المراجع

[أندريسين 2014] آندريسين، "سبب أهمية بيتكوين"،
http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters

[DNS/TCP] https://lists.dns-oarc.net/mailman/listinfo/tcp-testing

[فايز بقش 2013] فايز بقش 2013 وآخرين، "ألم أقل، معظم المكاسب: ICN القابل للنشر تدريجياً"، سيغكوم 2013

[غودسي 2011] غودسي وآخرين، "التسمية في هندسة تميل إلى المحتويات"، سيغكوم 2011

[هاستون 2013] دراسة DNS عبر TCP فقط.

http://www.circleid.com/posts/20130820_a_question_of_dns_protocols/
والخيوك التركيبية لعمليات dns

[ICANN 2013] "دليل تحديد تضارب الأسماء والتخفيف منه لمهنيي IT"،
https://www.icann.org/en/about/staff/security/ssr/name-collision-mitigation-05dec13-en.pdf

[كامينسكي 2004] د. كامينسكي، "توجيه الصوت والفيديو وSSH عبر الإنترنت"، بلاك هات 2004

[الجدوى] **الأقسام حول النطاقات وDNS**

http://www.afnic.fr/en/about-afnic/news/general-news/6391/show/the-internet-in-10-years-professionals-answer-the-afnic-survey.html

[موكابيتريس 88] ب. موكابيتريس وك. دانلاب، "تطور نظام أسماء النطاقات"، سيغكوم 88

[نيويوركر 2013]

http://www.newyorker.com/online/blogs/elements/2013/12/the-mission-to-decentralize-the-internet.html?goback=%2Egde_1430_member_5817512945197801473#%21

[RFC 881] ج.بوستيل، "جدولوخطة أسماء النطاقات"، نوفمبر 1983

[RFC 882] ب. موكابيتريس، "أسماء النطاقات- المفاهيم والتسهيلات"، نوفمبر 1983

[RFC 883] ب. موكابيتريس، "أسماء النطاقات- التنفيذ والمواصفات"، نوفمبر 1983

[RFC 1034] ب. موكابيتريس، "أسماء النطاقات- المفاهيم والتسهيلات"، نوفمبر 1987

[RFC 1035] ب. موكابيتريس، "أسماء النطاقات- التنفيذ والمواصفات"، نوفمبر 1987

[سبايغل 2014] http://www.spiegel.de/international/world/nsa-secret-toolbox-ant-unit-offers-spy-gadgets-for-every-need-a-941006.html

8. معجم المصطلحات

AI	الذكاء الاصطناعي
API	واجهة برنامج التطبيق
CCN	الشبكات المحورية للمحتويات
ccTLD	اسم نطاق المستوى الأعلى لرمز الدولة – وهو TLD يتم تعيينه إلى دولة معينة
DANE	التحقق من صحة الهيئات المسماة بحسب DNS
DDOS	رفض الخدمة المتوزع
DNS	نظام أسماء النطاقات- نظام تسمية الإنترنت
عمليات DNS DNSOPS	- مجموعة عمل تابعة لـIETF تهتم بمسائل عمليات DNS وأمور اخرى
DNSSEC	الامتدادات الأمنية لنظام أسماء النطاقات
DSL	خط المشترك الرقمي
E.164	توصية من ITU-T، بعنوان خطة ترقيم الاتصالات العامة الدولية، تحدد خطة الترقيم لشبكة الهواتف المتحولة العامة (PSTN) على مستوى العالم وبعض شبكات البيانات الأخرى
EDNS0	آلية الامتداد لـ [RFC 2671] DNS – معيار توسعة حجم وحقول مواصفات DNS الأصلي
ENUM	توجيه الرقم E.164- نظام لتوحيد نظام أرقام الهواتف الدولية لشبكة الهواتف المتحولة العامة مع مساحات عنونة وتحديد مساحات أسماء الإنترنت، لتوجيه مكالمة هاتفية مثلاً
FEDEX	فيديرال إكسبريس
FQDN	اسم نطاق مؤهل بالكامل
FTP	بروتوكول نقل الملفات
gTLD	اسم نطاق المستوى الأعلى – وهو TLD لا يتوافق مع رمز دولة
HTTPS	أمن بروتوكول نقل النص الفائق
IANA	هيئة أرقام الإنترنت المُخصصة
ICANN	مؤسسة الإنترنت للأرقام والأسماء المُخصصة
ICN	الشبكات المحورية للمعلومات
IEEE	معهد مهندسي الكهرباء والإلكترونيات
IETF	قوة مهمات هندسة الإنترنت

IP	بروتوكول الإنترنت
IPSEC	أمن بروتوكول الإنترنت
IPv4	بروتوكول الإنترنت الإصدار 4
IPv6	بروتوكول الإنترنت الإصدار 6
ITI	ابتكار تكنولوجيا المعرف – لجنة إستراتيجية تابعة لـ ICANN
LISP	بروتوكول فصل محدد المواقع/ المحدد [RFC 6830]
MIB	قاعدة معلومات الإدارة
MTU	وحدة نقل الحد الأقصى- حجم وحدة الحد الأقصى من البيانات التي يمكن نقلها، أو نقلها من دون تجزئة.
MX	تبادل البريد- نوع بيانات DNS يحدد تبادل البريد الذي يتعامل مع البريد لنطاق معين
NAPTR	مؤشر هيئة الأسماء- نوع بيانات DNS يستخدم بشكل واسع في الإرسال الهاتفي للإنترنت
NDN	شبكات البيانات المسمية
P2P	نظير إلى نظير
PKI	البنية التحتية الرئيسية العامة
RFC	طلب التعليقات- مذكرات توثق مسائل الإنترنت التقنية والتشغيلية
RIR	سجل الإنترنت الإقليمي- إحدى المنظمات التي تدير جميع وتسجيل موارد أرقام الإنترنت ضمن منطقة معينة من العالم. على سبيل المثال، ARIN، السجل الأمريكي لأرقام الإنترنت يتعامل مع كندا والولايات المتحدة والعديد من جزر الكاريبي وشمال المحيط الأطلسي.
Rsynch	بروتوكول التزامن عن بُعد- يزامن الملفات والأدلة مع الحد من نقل البيانات باستخدام تشفير دلتا.
RR	سجل الموارد- الوحدة الذرية للمعلومات في DNS
TSIG	توقيع المعاملة
TTL	الوقت للاستمرار
TXT	نوع سجل الموارد النصي في DNS الذي يسمح بالحقول النصية من التنسيق الحر
UDP	بروتوكول حزمة معلومات المستخدم- بروتوكول حزمة معلومات الإنترنت بلا اتصال
UI	واجهة المستخدم
URI	معرف المورد الموحد
URL	محدد موقع المورد الموحد
WIFI	الدقة اللاسلكية- معايير الشبكة اللاسلكية المحددة من قبل عائلة معايير IEEE 802.11

9. المساهمات من أعضاء اللجنة

يرجى الملاحظة أن جميع المساهمات هي منقولة بشكل حرفي كما تم تقديمها من قبل الأفراد.

9.1. مساهمة جيمس سينغ

الهندسة التقنية

المتسلل الإلكتروني في داخلي يحب الهندسة اللا مركزية. يمكن الجدال بأن العديد من "المشكلات السياسية" التي نعانيها اليوم ناتجة عن الطبيعة المركزية لـ DNS مع الجذر.

لذا فإن التكنولوجيا مثل نيمكوين أو نظام المعرفات اللا مركزية الأخرى تأسر اهتمامي.

ولكن ليس ثمة نظام معرفات لا مركزي ولكن منسق أعرفه تم استخدامه بشكل واسع. لذا سواء أعجبكم هذا أم لا، ما زال نظام DNS هو أحد أنظمة المعرف المنشورة التي لدينا. كما فعلنا في IETF، "الرموز العاملة" هي ما يفوز، وليس الأفضل تصميماً بالضرورة.

لا أؤمن بالجذر المتعدد، أو الجذر البديل. كما قلت في بيونيس آيريس، أنا أؤيد RFC 2826. الجذر المتعد، الجذر البديل وجميع المقترحات المرتبطة تنقل المشكلة السياسية إلى طبقة أخرى فحسب، ولكنها لا تحل المشكلة السياسية الأساسية. لاحظوا أني قلت مشكلة سياسية لأني لا أعتقد أن الجذر المتعدد يحل أية مشكلة تقنية على الإطلاق، بل إنها تزيد من التعقيد التقني في الحقيقة

ICANN

أدى DNS وطبيعته المركزية للجذر بشكل جزئي في تشغيل وظيفة IANA البسيطة الأصلية إلى أن تصبح ICANN المنظمة الكبرى التي أصبحت عليها اليوم.

لقد شاركت مع ICANN منذ أول اجتماع باريس في عام 1999، وشاركت في كل اجتماع تقريباً منذ ذلك الحين. على مدار تلك السنوات، ثمة أمور أتمنى لو فعلتها ICANN بشكل مختلف، أي أن مواقفنا ليست متوافقة دائماً.

ولكن ICANN هي "الرمز العامل" لتنسيق معرفات DNS. ربما ثمة تصاميم أفضل، وربما أبسط وأكثر أناقة (كما يرغب الهديد من أعضاء مجتمع IETF، يمكننا الرجوع إلى أيام جون بوستيل)، ولكن هذا هو الحال اليوم، والأهم من ذلك، فإنه ناجح رغم أنه يمكن أن يصبح أفضل. إن (ITU) البديل المقترح الذي نعرفه يعاني مشكلات أخرى أو ما هو أسوأ.Â

لذا أنا أؤيد ICANN لأنه أفضل نظام ناجح لدينا لتنسيق معرفات DNS والجذر.

توسعة DNS ونظامه إلى مجالات أخرى

بالتالي، لست مهتماً كثيراً بإعادة تصميم DNS أومقترحات بديلة لمعرفات التسمية. في النهاية، ينبغي وجود شخص ما، أو منظمة ما، للقيام بالتنسيق، وسنواجه نفس المشكلات السياسة من جديد.

أؤيد وأحب رؤية نظام DNS التركيبي (معايير DNS، عمليات الجذر، ICANN) الذي لدينا وتم تصميمه بالأصل لـ DNS وتطور للتوسع إلىمناطق أخرى (مثل RFID)، حتى يمكن ضم المزيد من المجتمع. بشكل ما، العمل الذي قمنا به في IDN هو ضمن مجموعة من مجتمع المستخدمين الذين يحتاجون إلى استخدام لغتهم الأصلية الخاصة في نظام DNS التركيبي، بدلاً من السماح لهم ببناء نظامهم التركيبي الخاص.

رغمأن البعض قد يجادلني بأنه إذا قمنا بـ IDN خارج نظام DNS التركيبي، كان النشر سيكون أسرع (مثلاً، راجع الكلمات الرئيسية الأصلية)، ومن رأيي أن IDN هو أفضل أيضاً لأنه جزء من نظام DNS التركيبي، حيث ثمة معايير مفتوحة جيدة التعريف وتطبيقات مفتوحة وشركات تضيف إلى تركتنا من DNS، وبشكل مشابه حماية مشتركي IDN ومستخدميها النهائيين.

بالتالي، لا أشعر بتأنيب الضمير، وأؤيد استكشاف كيف يمكننا توسعة DNS إلى معرفات لم يتم تصميمه لها بالأصل. غالباً ما يكون المهندسون الذين يصممون المعرفات جاهلون بالسياسة التي ترافق المعرفات، وخاصة إذا كانت مثل هذه المعرفات مكشوفة للمستخدمين النهائيين. يمكنهم تعلم بضعة أمور من تاريخ معرفات DNS في ICANN.

الأمور السياسية في الجذر

الأمور السياسية في ICANN، وعدد من يعتبرونها جزء من "حوكمة الإنترنت" تأتي من دورها في تنسيق مخادم الجذر.

لتزداد الأمور سوءاً، 11 من أصل 13 مخدم جذر مقرها في الولايات المتحدة، بسبب مصادفة تاريخية، ولكن هذا يجعل من فكرة وقوع ICANN تحت سيطرة الولايات المتحدة أسوأ، وخاصة في هذه الأيام بعد سنودين.

كلما يأتي أحد ويقول إن هذه الدولة أو تلك ينبغي أن تحظى بمخدم جذر، فإننا نرد باستخدام مبررات تاريخية أو تقنية تمنع التوسع إلى ما هو أكثر من 13 جذر.

يمكنني قبول التاريخ كمبرر.

ولكن ليس المبررات التقنية. إنه أشبه بعذر لأني لم أسمع بأية جهود جدية تبذلها IETF للتوسع إلى ما هو أكثر من 13 جذر. لهذا قلت أثناء اجتماع بيونيس آيريس أن بوسعي التفكير ببضعة حلول تقنية، تكفي كهوية على الأقل. لا يمكننا السماح لـ ICANN بمواصلة استخدام IETF/ المبررات التقنية كعذر للمشكلات السياسية التي تواجهها. ينبغي أن نتمكن من القول لـ ICANN، نعم يمكن القيام بذلك، ولكن القرار السياسي للقيام بذلك أم لا يرجع إليكم.

بالإضافة إلى ذلك، والأهم من ذلك، تشغيل مخادم الجذر ليس مبالغ فيه.

امتلاك جذر لا يعني أن هذه الدولة أو تلك ستمتلك السيطرة الفورية على الإنترنت. في الواقع، هذا ممل مثل جذر أنيكاست. رغم أنه إذا لم يتبع مشغل الجذر بعض الممارسات المثلى لتشغيل مخدم الجذر (مثل RFC 2010 وRFC 2870)، فقد يؤدي هذا إلى أضرار شديدة بالإنترنت.

الأرجح أن معظم المهندسين سيفهمون ما قلته أعلاه، ولكن معظم أعضاء ICANN لن يفهموه.

لذا ثمة اعتبارات عند اختيار مشغل مخدم الجذر، لأن هذا أساسي لاستقرار معرفات الإنترنت، ومعظمها مبني على الثقة. ولكن الثقة ليست مشكلة هندسية، سواء أعجبكم هذا أم لا.

- جيمس سينغ

http://chineseseoshifu.com/blog/dnspod-in-china.html

سبب فائدة DNSPod في الصين رغم "تقسيمها" الـ DNS.

9.2. قرار DNS وسلوك تطبيقات قائمة البحث- جيف هاستون

لا شيء- لا تقوم بأي بحث DNS

أبداً- تبحث عن اسم القاعدة، ولكنها لا تطبق قائمة البحث

قبل- تطبق قائمة البحث، وإذا كانت النتيجة NXDOMAIN، تبحث عندها عن اسم القاعدة

بعد- تبحث عن اسم القاعدة، وإذا كانت النتيجة NXDOMAIN، تطبق عندها قائمة البحث

دائماً- لا تبحث عن اسم القاعدة- بل تطبق قائمة البحث فحسب

سلوك مكتبة مقرر DNS لنظام التشغيل الأساسي

النظام	مطلق مخدم.	ملصق فردي مرتبط مخدم	ملصق متعدد مرتبط www.server
MAC OSX 10.9	أبدًا	دائماً	أبدًا
Windows XP	أبدًا	دائماً	بعد
Windows Vista	أبدًا	دائماً	أبدًا
Windows 7	أبدًا	دائماً	أبدًا
Windows 8	أبدًا	دائماً	أبدًا
FreeBSD 9.1	أبدًا	قبل	بعد
Ubuntu 13.04	أبدًا	قبل	بعد

سلوك المتصفح على منصات ويندوز وماك

MAC OSX 10.9

	مخدم.	مخدم	www.server
Chrome (31.0.1650.39 beta)	أبدًا	دائماً	قبل
Opera (12.16)	أبدًا	دائماً	أبدًا
Firefox (25.0)	بعد*	دائماً	بعد*
Safari (7.0 9537.71)	لا شيء**	لا شيء**	لا شيء**

* سابقة مضافة إلى "www."، ثم محاولة إضافة سابقة إلى "www". وكذلك إلحاق قائمة البحث

** يبدو أن Safari يدرك TLDs ولا يقوم بعمليات بحث DNS عندما لا يكون الاسم هو TLD

	مخدم.	مخدم	www.server
Explorer (11.0.900.16384)	لا شيء	لا شيء	أبدًا
Firefox (25.0)	أبدًا*	دائماً	أبدًا
Opera (17.0)	لا شيء	لا شيء	لا شيء**
Safari (5.1.7 7534.57.2)	أبدًا*	دائماً***	أبدًا

* سابقة مضافة إلى "www"

** يدرك OPERA الـ tlds المفوضة، ولا يسأل إلا عندما يكون الملصق الأخير هو TLD

*** سابقة مضافة إلى "www" ولاحقة إلى ".com"

9.3. ملاحظات حول مساهمة الاتساق والانحراف- جيف هاستون

إذا رجع المرء إلى أصول نظام أسماء النطاقات، سيجد ما يسمى "ملف المستضيف" كمحاولة مبكرة لإضفاء الأسماء المستخدمة من البشر إلى سياق شبكات الكمبيوتر. استخدمت ARPANET نموذج تسمية عقدة شبكة حيث كانت كل عقدة متصلة ذات ملف تهيئة، ملف المستضيف، يحتوي على أسماء عقد ARPANET الأخرى، وعناوين البروتوكول لكل عقدة. لم يكن ثمة اتساق مطبق على نطاق هذه الحالات المتعددة من ملفات المستضيف هذه على نطاق مجموعة العقد المتصلة بواسطة ARPANET، ولا كان، آنذاك، ثمة وسيلة لتوزيع نسخة عن ملف المستضيف على نطاق الشبكة. كانت خدمة ملف المستضيف هذا هي توفير أسماء ودية للبشر مكان عانوين مستوى البروتوكول الأكثر تبلداً. استطاع المستخدمون تحديد عقد الشبكة بواسطة اسمها الرمزي، والذي كان يُترجم عندها إلى عنوان ثنائي خاص بالبروتوكول عن طريق بحث في ملف المستضيف. مع نمو ARPANET، ازداد أيضاً حجم ونسبة تحديث ملف المستضيف وارتفعت النفقات الأساسية لصيانة مستضيف محلي دقيق أيضاً. تم تحديد معايير تنسيق ملف المستضيف (RFC952) وتم تعريف خدمة ملف مستضيف مركزي (RFC953) يمكنها الحلول محل العديد من النسخ المحلية للملف المستضيف.

ثم تم استبدال ذلك بنظام أسماء النطاقات (DNS)، المحدد بالأصل في عام 1983 في RFC 882 وRFC 883. كان يتم الحفاظ على آلية ترجمة اسم، محدد على أنه سلسلة ودية للبشر، إلى عنوان خدمة خاصة بالبروتوكول عن طريق النقل من ملف المستضيف إلى DNS.

ثمة عدد من الخصائص لمساحة المعرف هذه، ومن بينها الملاحظة بأن DNS يوسع مساحة اسم مناسبة للاستخدام في حوار بشري، وفي الوقت نفسه الاعتراف بهيكل رسمي كافٍ للسماح بالتلاعب بالأسماء من برامج كمبيوترية بشكل حتمي. إن مساحة أسماء DNS هي مساحة هيكل هرمي تسمح بالبحث في مساحة الأسماء بفعالية عن مطابقة دقيقة، وفي الوقت نفسه تسمح بإطار عمل للإدارة الموزعة لأسماء المساحات. ما دام يتم تجنب تضارب الملصقات ضمن أية منطقة فردي لهرمية أسماء DNS، يمكن تجنب تضارب الأسماء ضمن مساحة أسماء DNS الإجمالية، مما يسمح بإدارة تميز الأسماء بجاهزية ضمن سياق DNS. إن DNS هو مرن من ناحية وظيفة التوجيه، ويمكن استخدامه للتوجيه من مساحة اسم هيكلي إلى أي شكل آخر من موارد الأسماء تشير إليها خدمتنا. إن الهدف من DNS أن يكون متسقاً، من ناحية أنه نظراً لإدخال اسم متسق في DNS، ينبغي أن توفر الاستعلامات حول ذلك الاسم نفس الرد على نطاق مواقع متنوعة من المستعلم والأوقات المتنوعة للاستعلام. يسمح هذا بالاتساق المرجعي، من ناحية أنه يمكن تبادل اسم DNS بين الأطراف والإشارة إلى مورد متسق من موقع الخدمة. ليس الهدف أن يستبدل DNS نظام دليل أو نظام بحث. إذا كان ثمة مطابقة دقيقة للاسم الذي يتم الاستعلام عنه في DNS، ستكون نتيجة استعلام DNS هي القيمة الموجهة بسبب الاستعلام، وإلا ستكون نتيجة الاستعلام هي فشل بالمطابقة.

خضع استخدام هذا النموذج من مساحة أسماء DNS كمساحة أسماء المعرفات لدعم الواجهة البشرية مع الشبكة للعديد من التغييرات، وبشكل رئيسية رداً على نمط الاستخدام البشري للمعرفات في الحوار. إننا نميل إلى استخدام المعرفات بأشكال أقل دقة، وبأشكال تتضمن عناصر من السياق المحلي تستخدم لغات ونصوص محلية، وعلى مدار الزمن، أصبح دور DNS كشكل من الواجهة البشرية مع موارد وخدمات الشبكة متضمناً في جهود دعم الواجهات التي تعمل بشكل "طبيعي" أكثر للاستخدام البشري.

اقترح RFC1034 استخدام شكل من الاختصار بالكتابة في مواصفات أسماء DNS، حيث يتم اعتبار الأسماء التي لا تنتهي بتذييل '.' على أنها "أسماء مرتبطة"، وكما هو مبين في RFC1034، "تظهر أغلب الأسماء المرتبطة على واجهة المستخدم، حيث يتنوع تفسيرها من تطبيق إلى آخر". بشكل نموذجي، شمل مثل هذا التفسير المحلي الجمع بين قائمة البحث المحلية من لواحق الملصق، مما سمح للمستخدم بتحديد الجزء المبدئي من اسم النطاق، والاعتماد على التطبيق المحلي أو روتينات برمجيات قرار الاسم لإضافة لاحق معرف محلياً لتشكيل اسم DNS مكتمل.

تم التقدم بهذا النوع من الإطباق الانتقائي لمساحة معرفات DNS عن طريق استخدام لواحق الاسم خطوة إضافية في واجهة المستخدم التي توفرها متصفحات الويب، حيث كانت الممارسة الشائعة مع متصفحات الويب هي نقل مكون معرف DNS لـ URL وتطبيق تحويل اسم من الإضافة لبداية السلسلة "www." وإضافة لاحقة معرفة محلياً (غالباً ما تكون ".com"). بهذا الشكل، يصبح المعرف الذي حدده المستخدم واسم المعرف المستخدم في استعلام DNS اللاحق مرتبطان، ولكن ليسا متشابهين بالضرورة.

تم توسعة هذا الاستخدام لتحويل الاسم المحلي بحيث تم توجيه معرفات تشكلت من نصوص لغات عدا عن US ASCII إلى DNS (IDNs: RFC5891). كانت هذه عملية محددة بوضوح حيث يتم تحويل المعرف الذي أدخله المستخدم إلى سلسلة ملصق مشفرة تشكل استعلام DNS. في هذه الحالة، يكون التحويل محدداً بدقة، بحيث تهدف التطبيقات المتعددة لمعيار IDN إلى دعم نظرة متسقة لتوجيه معرفة في نص معين إلى شكل اسم DNS مشفر.

ارتقاء آخر بتنقية نموذج التفاعل البشري هو توحيد مصطلحات البحث وURLs كمدخلات في المتصفحات. في هذه الحالة، إذا لم يستخدم المستخدم المواصفات الكاملة لـ URL المتصفحة، سيحاول المتصفح تأريخها.

9.4. مساهمة من بول فيكسي

أنيكاست العالمي لمنطقة الجذر

نظرة عامة

إننا نقترح أن تقدم IANA عدة نماذج إضافية من منطقة جذر DNS، للسماح بأنيكاست عالمي والأبحاث التشغيلية. "أنيكاست العالمي" ضمن هذا السياق يعني منطقة جذر تبني ذروة سجلات NS الخاصة بها مخدمي أسماء اثنين فقط، والتي يمكن أن تستضيف عناوينها "المعروفة جيداً" (كما هي مبينة في سجلات A وAAAA) من قبل أي أحد. "الأبحاث التشغيلية" ضمن هذا السياق تتضمن الاختبار العام واسع النطاق لخدمة اسم جذر IPv6 فقط والاختبار العام واسع النطاق لتأثيرات تضارب "gTLD الجديد". يعامل هذا المنهج خدمة اسم الجذر على أنها خدمة غير خاضعة للإدارة بدلاً من خدمة خاضعة للإدارة.

الخلفية

لا يمكن نشر أنيكاست العالمي لمنطقة الجذر بشكل آمن ومسؤول قبل ظهور DNSSEC، لأنه من دون DNSSEC، يمكن تهيئة أي مخدمة مستجيب ببيانات DNS اعتباطية تتضمن TLD جديد أو TLD حالي تمت إعادة تفويضه. مع DNSSEC، أصبح من الممكن الآن لمشغلي مخدم الاسم المتكرر تهيئة التحقق من صحة DNSSEC، بحيث يجب أن تكون أية معلومات gTLD مسموعة من مخدم اسم جذر أنيكاست عالمي معتمدة من قبل IANA كما تشير تواقيع DNSSEC المصنوعة مع مفتاح توقيع منطقة جذر IANA (أو ZSK).

تتضمن الانتقادات الموجهة لنظام مخدم اسم الجذر الحالي والتاريخي انعدام المقاومة أمام هجمات DDoS، مع التنويه بأنه حتى مع أنيكاست واسع النطاق الحالي من كل مشغل مخدم اسم جذر، ما زال ثمة بضعة مئات من مخادم الأسماء في العالم التي يمكنها الرد بحزم على منطقة جذر DNS. كما أننا نخشى أن قابلية وصول نظام مخدم اسم الجذر هي متطلبة حتى للاتصالات المحلية المحضة، وإلا لن يكون بوسع العملاء المحليين اكتشاف الخدمات المحلية. في نظاممو زع بحجم العالم مثل الإنترنت، ينبغي أن تكون الخدمات الحرجة ذات توزيع جيد للغاية.

التفاصيل

ثمة العديد من الأشكال المتباينة التي ينبغي إنشاءها. أولاً، أنيكاست العالمي الأساسي سيسمح لأي مشغل مخدم اسم بتصوير الحركة الموجهة نحو نظام مخدم اسم الجذر والرد عليها محلياً. ستستخرج IANA وتوقع رقمياً (بواسطة DNSSEC) نسخة إضافية من منطقة الجذر ذات مجموعة مختلفة من سجلات NS في ذروتها. ستحدد سجلات NS مخادم الأسماء التي لم يتم تعيين عناوينها إلى أي مشغل مخدم اسم جذر (RNSO)، بل تم احتجازها من قبل IANA للاستخدام من قبل أي أو جميع الأطراف المعنية. ستطلب IANA تخصيص مايكرو البنية التحتية من RIR (مثل ARIN أو APNIC)، كعدة سوابق IPv4 24 بيت وعدة سوابق IPv6 48 بيت، للاستخدام في أنيكاست عالمي لمنطقة الجذر.

متباين آخر لمنطقة الجذر الحالية سيوفر أنيكاست عالمي كما هو مبين أعلاه، ولكنه سيحدد مخادم الاسماء ذات اتصال IPv6 فقط (المشار إليها بوجود سجلات AAAA) وبلا اتصال IPv4 (المشار إليها بغياب سجلات A). سيسهل هذا المتباين من الأبحاث التشغيلية لشبكات IPv6 فقط.

المتباين الثالث لمنطقة الجذر الحالية سيوفر أنيكاست عالمي كما هو مبين أعلاه، ولكنه سيتضمن التفويضات لجميع gTLDs الجديد المعروفة، بما في ذلك تلك غير الجاهزة للتفويض (مثلCORP. وHOME.). سيتم تفويض gTLDs الجديدة هذه إلى مخدم اسم بتشغيل من IANA نفسها، لأغراض القياس. سيتم تعيين سجلات A وAAAA متغيرة لكل gTLD جديدة، وستصل عناوينها إلى مخادم الويب التي تشغلها IANA لأغراض القياس.

التأثير

نظراً للطبيعة الهرمية لتوجيه الإنترنت، يمكن الإعلان عن كتل عنوان أنيكاست على عدة مستويات. قد تمتلك آلة افتراضية (VM) تعمل على كمبيوتر محمول عملية مخدم الأسماء الخاصة بها التي تصغي إلى العناوين المعروفة جيداً المناسبة، وفي هذه الحالة، لن تغادر أية استعلامات خدمة اسم جذر تلك الآلة الافتراضية. كما يمكن للكمبيوتر المحمول نفسه تصوير الحركة إلى الخارج المستهدفة إلى تلك العناوين المعروفة جيداً، والتي ستخدم الآلات الافتراضية الأخرى أو العمليات التي تعمل على ذلك الكمبيوتر المحمول. قد يمتلك التدفق العلوي لجهاز التوجيه اللاسلكي لذلك الكمبيوتر المحمول مخادم تصغي إلى تلك العناوين، وفي هذه الحالة، لن تغادر أية استعلامات خدمة اسم جذر تلك الـLAN اللاسلكية. قد يشغل ISP مخادم تصغي إلى تلك العناوين المعروفة جيداً، لخدمة أي وجميع العملاء الذين لا يشغلون مخادم خاصة بهم. في النهاية، من المتوقع من الإنترنت العالمي امتلاك العديد من المشغلين الذين يعلنون عن الطرق إلى كتل العناوين المعروفة جيداً هذه، وليس أقلها مشغلي مخدم أسماء الجذر الاثنا عشر الحاليين.

سيكون التأثير الإيجابي لهذا المرونة المحتملة الأكبر، وتخفيف التأخير في خدمة أسماء الجذر. بينما سيكون التأثير السلبي هو تخفيض القدرات التشخيصية، وازدياد ضعف "توجيه الطريق" أو "الاختطاف" في حركة خدمة أسماء الجذور. من الضروري بأي حال من الأحوال أن يصبح التحقق من صحة DNSSEC شائعاً من أجل الحد من محصلة هذا النوع من الاختطاف. نريد أن تكون محصلة المهاجم هي "فقدان الضحية لخدمة أسماء الجذر" بدلاً من "رؤية الضحية لمساحة أسماء DNS مختلفة".

أمثلة

تبين الأمثلة التالية مجموعة ذروة سجل NS لكل متباين منطقة جذر، بما في ذلك تعليق العنوان. ستكون هذه البيانات مشمولة في متباين منطقة الجذر قبل توقيع DNSSEC، كما سيتم نشرها كملف "تلميحات الجذر". كما ستكون البيانات الظاهرة في iana-servers.net موجودة في منطقة iana-servers.net الحقيقية. ستتطلب هذه الأمثلة أربعة تخصيصات مايكرو IPv4 وستة تخصيصات ماكيرو IPv6.

المتباين 1: أنيكاست العالمي

. IN NS anycast-1.iana-servers.net.

. IN NS anycast-2.iana-servers.net.

$ORIGIN iana-servers.net.

anycast-1 IN AAAA 2001:?:1::1

anycast-1 IN A ?.?.1.1

anycast-2 IN AAAA 2001:?:2::2

anycast-2 IN A ?.?.2.2

المتباين 2: أنيكاست العالمي لـ IPv6 فقط

. IN NS v6only-1.iana-servers.net.

. IN NS v6only-2.iana-servers.net.

$ORIGIN iana-servers.net.

v6only-1 IN AAAA 2001:?:3::1

v6only-2 IN AAAA 2001:?:4::2

المتباين 3: أنيكاست دراسة تضارب gTLD

. IN NS gtldstudy-1.iana-servers.net.

. IN NS gtldstudy-2.iana-servers.net.

$ORIGIN iana-servers.net.

gtldstudy-1 IN AAAA 2001:?:5::1

gtldstudy-1 IN A ?.?.5.1

gtldstudy-2 IN AAAA 2001:?:6::2

gtldstudy-2 IN A ?.?.6.2

10. الملاحق

10.1. مواد LISP

10.2. مواد API هوفمان