شركة الإنترنت للأسماء والأرقام المخصصة

تقرير لجنة إبتكار تقنية المعرّف

15 أيار 2014 - نهائي

جدول المحتويات

1. مقدمة

تم تعيين لجنة إبتكار تقنية المعرّف (ITI) من قبل شركة الإنترنت للأسماء والأرقام المخصصة (ICANN) مع الأهداف التالية:

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

تم إختيار أعضاء اللجنة خلال شهر أيلول وتشرين الأول 2013 وتم أختيار پول موكاپيتريس رئيساً لها. وعمل كل الأعضاء كأفراد مع إنتماءاتهم لأغراض تعريفية وهم:

- جاري آركو Jari Arkko - رئيس فريق عمل هندسة الإنترنت (IETF)
- ريك بويڤي - من مركز بحوث توماس ج. واتسون في IBM.
- آن- ماري إيكلوند- لويندير - مديرة الأمن، مؤسسة البنية التحتية للإنترنت
- جيوف هوستون - كبير العلماء، مركز معلومات شبكة آسيا والمحيط الهادي
- جيمس سينغ- المدير التنفيذي لمؤسسة زودياك القابضة Zodiac Holdings
- پول ڤيكسي - المدير التنفيذي لشركة Farasight Security
- ليكسيا زانغ - رئيس قسم (وكالةً) علوم الحاسبات في جامعة كاليفورنيا في لوس أنجلوس

تم عقد إجتماعات مباشرة وجهاً لوجه في مقر فريق عمل هندسة الإنترنت IETF في فانكوڤر (في شهر تشرين الثاني 2013)، وفي أجتماع ICANN في بوينس آيريس (في شهر تشرين الثاني 2013) وفي مكاتب ICANN في لوس أنجلوس (في شهر كانون الثاني 2014). كان إجتماع بوينس آيريس مفتوحاً الى عامة الناس وقد تم عرض خلاصة لأنشطة اللجنة من خلال جلستين عبر الإنترنت (webinars) في شهر كانون الثاني 2014. علاوةً على النقاشات الجارية من خلال البريد الإلكتروني، وما الى ذلك. ومنذ شهر شباط 2014 فصاعداً، نشرت نسخ مسودة من التقرير وأصبحت متوفرة للجميع لأجل التعليقات العامة.

يود رئيس اللجنة التقدم بالشكر الى كافة أعضاء اللجنة لآرائهم ورؤاهم وكذلك الى ICANN للدعم الذي قدمته للجنة. وشكراً أيضاً الى إيليس غريتش وآليس هانسين من ICANN واللذين ساهما بأفكار ودعم لكافة أعمال اللجنة.

2. أستراتيجية اللجنة

لم يأتِ عنوان اللجنة من قبيل صدفةً. لقد تم توسيع نطاق العمل لما هو أبعد من نظام أسم النطاق DNS بحد ذاته إعترافاً بالأهمية المتزايدة للمعرّفات بكافة انواعها للإنترنت، علاوةً على دور ICANN في إدارة معرفات أخرى. وتتضمن القائمة الجزئية من المواضيع الهامة الحالية التي تعمل عليها ICANN مايلي:

- أسماء النطاقات
- أرقام النظام المستقل ذاتياً
- عناوين الإنترنت لبروتوكول الإنترنت - الاصدار الرابع IPv4
- عناوين الإنترنت لبروتوكول الإنترنت - الاصدار السادس IPv6
- عنوان الإرسال المتعدد
- أرقام المنافذ
- أرقام البروتوكول
- سجل المعرّف الموحد لمصدر المعلومات URI
- قاعدة معلومات الإدارة MIB
- قاعدة بيانات المناطق الزمنية

ومع ذلك، وتزامناً مع هذا التوسع، فإن الإطار الزمني لعمل اللجنة قد تم تقليصه من سنة واحدة كما حدد مسبقاً الى مايقارب الستة أشهر. وكان لهذا أثراً كبيراً على التركيز الخاص بنظام أسم النطاق وبصورة أكبر مما كان يؤمل.

ولأجل الإستفادة القصوى، إعتمدت اللجنة المبادئ التالية:

- حاول توثيق كافة الأفكار التي طرحت ولكن ركّز على القليل منها
- أبحث عن متجهات قوة محددة (مثل توسيع الإنترنت، والتوجهات الخاصة بهندسة المُعامِل Processor)
- أبحث عن الإحتياجات "الأساسية والأكثر إلحاحاً"
- تجنب التركيز على "المجالات التي نوقشت كثيراً" (مثل نشر DNSSEC، الإستراتيجيات الحالية لتضارب الأسماء) وإبحث عن أفكار مبتكرة

الغرض الأساسي للجنة هو إثراء عملية التخطيط الإستراتيجي لـ ICANN. ورغم أن اللجنة تأخذ بعين الإعتبار الأفكار القريبة من الاحتياجات التشغيلية لـ ICANN، إلا إنها 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. وتثير بعض الأفكار تساؤلات تتعلق بالسياسة والتي لم تتناولها اللجنة بما هو أبعد من الإشارة إليها فقط.

واخيراً، وبالنظر للقدر الكبير من الأنشطة في مجال معرّفات الأنظمة المصنّفة، فإن اللجنة أستطاعت بالكاد تناول عينة بسيطة من هذا المجال. وينبغي ألا يفترض القارىء بإن اللجنة كانت على علم بكافة الأنشطة الجارية، أو أن الأفكار التي لم تتم مناقشتها هنا لايعني بانها ذات أهمية أقل.

3. خارطة الطريق

لازالت المعرّفات من المسائل الأكثر أهميةً في مجتمع الإنترنت. وعلى المدى القصير ستكون هناك نطاقات مستوى أعلى (TLDs) جديدة فعّالة على شبكة الإنترنت. ويتطلع حسابك الشخصي على الفيسبوك لأن يكون إعتماد تسجيل الدخول الوحيد لك على الإنترنت وكما هو الحال في حسابك على صفحة الغوغل. وعلى المدى الطويل، فلمجتمع البحوث الكثير من المشاريع المختلفة بما في ذلك مشاريع التشبيك المحوري للمحتوى (CCN, Content Centric Networking)، والتشبيك المحوري للمعلومات (ICN, Information Centric Networking)/ ومشروع تشبيك البيانات المسماة (NDN, Named Data Networking) وغيرها الكثير من المشاريع المتنوعة. وفي الوقت الذي لايتفق مجتمع البحوث على أسم لهذا المجال، إلا إنهم على أتفاق تام بأنه ينبغي تعريف المحتوى بأسم وليس بعنوان أو موقع وأن يتم أنتهاز أية فرص مؤاتية بخصوص الإحتفاظ بأي محتوى. وقد دعت مشاريع مقترحة أخرى على أن تكون الأسماء الصريحة التامة هي الموجة المستقبلية وإنه ينبغي أن تكون الأسماء المعتمدة ذاتياً بمثابة الأساس لأي نظام جديد.

إن المعرّفات ذات أهمية مركزية لأي شبكة فيما يخص تعريف المحتويات الخاصة بها لكافة المكونات الأخرى للشبكة. بالإضافة الى ذلك، فإن الشبكات الحديثة ليست بنطاق منفرد متجانس، ولكن تم بنائها على شكل مزيج مكوّن من عدد من التقنيات وإن هناك شرط لتحديد هوية المناطق والعوالم أو المجالات الموجودة ضمن هذا المزيج. وظيفة تحديد الهويات هذه تتم بعدد من الطرق. ففي سياق الإنترنت، واحدة من طرق تحديد هوية العوالم أو المجالات الأكثر وضوحاً هي أسم النطاق الذي تم تصميمه بشكل هرمي. وترتبط مع أسم المجال هذا وظيفة تحديد الهوية التي بإمكانها تحديد أسم النطاق وهويات أخرى (مثل عناوين بروتوكل الإنترنت IP على سبيل المثال). عندما ننظر الى خارطة تحديد المعرّفات نحتاج أن نكون على دراية بالتمييز بين مجال المعرّف ووظيفة تحديد الهوية، وننظر الى خارطة طريق لكل منهما على حدة.

ففي الإنترنت الحالية، حددت اللجنة عدة عوامل من شأنها أن تؤدي الى توسيع إستخدام نظام أسم النطاق DNS وكثير من العوامل الاخرى المتعددة والتي من شانها أيضاً المساعدة في توسيعه. هذه العوامل ليست كلها تقنية ويبدو الصراع مع مثل هذه القضايا أمراً طبيعياً أكثر مما يمكن أن يوصف بانه فقط مظهر من مظاهر اللياقة الظاهرية.

<u>العوامل الحالية للتوسع</u>

- يتمتع نظام DNS بميزة موروثة وهي أنه يمكن تنفيذه في كل جهاز يكون بتماس مع الإنترنت. وأي نمو بسيط في القاعدة الحالية من شأنه أن يؤدي الى توسيع إستخدامه. فمثلاً، التطبيق الذي يود عبور مايسمى بالجدران النارية (firewalls) والذي ينبغي حفظه في فضاء الإنترنت سيجد نظام DNS كقاعدة قائمة.
- وستحاول نطاقات المستوى الأعلى إعطاء قيمة كبيرة لعلاماتها التجارية. وحيث أن هناك الكثير من التشكيك والبحث في المجتمع التقني فإن أكثر من ألف علامة تجارية جديدة ستكافح من أجل أن تزدهر، وعلى الأرجح سيكون هناك الكثير من الإبتكار والعديد من المفاجآت.
- إن إنشاء إمكانيات جديدة مثل إمكانية الأمن الخاصة بالإمتدادات الأمنية لنظام أسم النطاق (DNSSEC) أو المصادقة المستندة على DNS للوحدات المسماة (DANE, DNS-based Authentication of Named Entities)، من شأنه أن يعمل على تعزيز المزيد من الأستخدام.
- ويمكن للبيانات الجديدة لنظام DNS أن توسع أستخدامها وخصوصاً عندما تربط بالأمتدادات الأمنية لنظام أسم النطاق DNSSEC لضمان صحتها وموثوقيتها. دعا أحد أعضاء اللجنة الى نشر ما أسماه "تاريخ الميلاد" وهو االفاصل الزمني الذي عنده تم تغيير تفويض أمين السجل أو النطاقات، كمعلومات أساسية تخص شهرة وصيت اللجنة. وقد أستخدمت مشاريع أخرى نظام DNS كسجلات لقوائم العناوين والانظمة المستقلة ذاتياً... الخ. وقد حددت ICANN إستخدام بعض العلامات التجارية في أسماء النطاقات وقد يكون السجل مناسباً في فترة تشيغله وخصوصاً عندما يتم تصنيف الصفحات يكون مرتباً وفق عدة أبجديات. وقد يكون تطبيق قواعد البيانات تلك إما عاماً أو خاصاً.
- يعني مصطلح "إنترنت الأشياء Internet Of Things" عدة أشياء للعديد من الأشخاص، ولكنه عادةً يشمل عدداً كبيراً من العناصر في واحدة أو أكثر من قواعد البيانات الموزّعة. وقد تم إقتراح DNS كحجر أساس في عدة هياكل ونماذج إنترنت الأشياء (IOT)، من خلال كونه كنظام DNS عام وكواحد أو أكثر من قواعد بيانات DNS الخاصة. تود اللجنة لو كان لديها

الوقت اللازم لأستكشاف هذه المسألة على نحو أكمل وتوصي بالمزيد من الدراسة وتؤمن بأن نظام DNS قد يكون له دوراً بطريقة أفضل.

العوامل الحالية للإنكماش

- إن DNS هومعيار موروث، ولكن ذلك أيضاً يشكل عائقاً أيضاً في منطق DNS المتجسد في نقاط ولوج WIFI وموديمات خط المشترك الرقمي (DSL) والكيبل والجدران النارية (firewalls) وأجهزة التوجيه، وإن قاعدة البرامجيات للإنترنت غالباً ما تحد من نطاق الاستخدام وتقيد الابتكار. غالباً ما تكون تطبيقات DNS أقل من حالة الإكتمال، أو محدّث أو ممتثل مع المعايير. لقد أعاقت هذه المسائل من تنفيذ DNSSEC وجعلت تنفيذ أية مظاهر أو أنواع من أنظمة DNS مثيرة للمشاكل. ويؤدي هذا إلى تصميم ممارسات مثل الحد من كل إستخدام لمعالجة وكتابة السجلات. وهذا التحجّر لايقتصر فقط على DNS.
- ثمّة إهتمام تجاري بالسيطرة على (" إمتلاك") صفحة البحث و/أو فضاء المعرّف. الإهتمام هنا هو لمعرفة نية المستخدم في الشكل الحر الأصلي والحفاظ عليه مخبّئاً عن فضاء الإنترنت المفتوح. لاحظت اللجنة إن الميل الى الأجهزة ذات الرموز الثابتة لخدمة معينة لنظام DNS وكذلك إمتدادات الملكية كمسار للتجزئة.
- يفضل المستخدمون واجهات أكثر فاعليةً. وبدلاً من الدخول على أسماء أنظمة DNS، فإن المستخدمين والمتقدمين بالطلبات غالباً ما يتبنّون أسلوب البحث وآليات أخرى للوصول الى معلومات محددة. وعلى سبيل المثال، يعتبر شريط محدِّد المصدر الموحد(URL) في المتصفحات، أداة بحث تستعمل على نطاق واسع. واليوم تعتبر الواجهة الاكثر شيوعاً وأستخداماً هو جهاز الهاتف المحمول والتي لا تحبذ الطباعة. تؤدي تقنيات تمييز الأصوات وانواع اخرى من تطبيقات الذكاء الصناعي (AI, Artificial Intelligence) في شريط التصفح الى عدم التطابق بين البائعين المختلفين. وكمثال على ذلك، قام جيوف هيوستون أحد أعضاء اللجنة (شاهد المساهمة) بتجربة لاحظ فيها تأثر البحث عن كلمة"Geoff. Huston" من خلال عدة متصفحات حيث لاحظ لا وجود لأي إتساق بين الجهات المزودة. يمكن قبول مثل هذا الإفتقار الى الإتساق في متصفح البحث عندما يتوقع من مستخدم الإنترنت أن يهتم ويراعي المعلومات الناتجة من ذلك البحث، ولكنه من الممكن أن يكون هذا النقص خطراً في ملفات التكوين في الأنظمة - وواحدة من المخاوف هي تكرر تضارب الأسماء.

كان رأي اللجنة أنه رغم أن استخدام DNS قد يضعف تدريجياً من واجهة المستخدم، إلا إنه من المرجح أن يظل كبنية تحتية أساسية. أحد التشبيهات هو أن DNS ليس عبارة عن ورق يقف بمواجهة هجمات الكتب الإلكترونية، بل بالأحرى مجموعة تعليمات كمبيوترية يمكن الولوج إليها من خلال لغات ذات مستوى أعلى.

وقد أختلفت الآراء بخصوص فيما لو كان من الممكن أو من المستحسن السعي لإحداث قفزة في نظام DNS أو إعادة هيكلته. وقد تمت مناقشة التقنية في قسم "أساسيات DNS" في هذا التقرير. هناك ثمة تساؤل بخصوص السياسة حول فيما لو يتعيّن على ICANN أن تحاول الحفاظ على نظام DNS وأن تعمل على توسيعه. إن كان ينبغي ذلك، فكيف يتسنى لأحدهم الحصول على هيكل متسق إعتماداً على مختلف وجهات النظر لدوائر كل من ICANN و فريق عمل هندسة الإنترنت IETF (حيث يفترض بإنه تم تنفيذ العمل) ووجهات أخرى في مجال الإنترنت؟

المدى الأطول

مجموعة واحدة من الأفكار بخصوص المدى الطويل هو نموذج بيانات التشبيك المسمّاة. والفكرة الأساسية في مجمل هذه الأفكار هي الوصول الى المحتوى من خلال الأسم ومن خلال التحقق بطريقة رقمية في كل مكان وإنتهاز كافة الفرص الممكنة ومخطط لجريان العمليات الذي تتم وفقه محتويات الطلبات والردود. يمكن عرض نموذج لتوجيه الإستفسارات أحياناً فقط بأستخدام تسلسل هرمي للمقاطع الأطول التي تطابق قرارات التوجيه التي تثير شكوكاً غير قابلة للقياس. وفي كل الأحوال يتم تنفيذ البرامجيات والأجهزة وإجراء عدة أختبارات للشبكة. من التطبيقات الأكثر وضوحاً هي توزيع المحتوى إلا إن المؤيدون يزعمون إن النموذج مناسب للسيطرة على العملية وعلى الشبكات المتحركة والخ.

وبمعنى أن نظام DNS كان هو الأول من الأنظمة البديلة التي أستخدمت لتنقية ICN، تماماً مثل المناهج الأخيرة [فياض بقش 2013] التي تحاول الحفاظ على الأجزاء الأهم من نموذج ICN. تكمن الأهمية هنا في عين الناظر.

يسترجع DNS البيانات بالأسماء. لم يكن القصد التوجيه بواسطة الأسم ولكن بدلاً من ذلك يستخدم طبقة عنونة الإنترنت ليجعل من السهل الوصول الى المحتوى، وهذا الأمر يعمل على إصلاح بعض الأمورمثل مشكلة القياس المركزي للشبكات المحورية للمعلومات ICN.

يُعرف DNS بصورة واسعة على أنه مركبة لتوجيه الفيديو [كامينسكي 2004] ويحظر توجيه الولوج من خلال إستفسارات DNS التي تتم قبل التحقق من الصحة من قبل بعض نقاط ولوج WIFI. (بحث "توجيه DNS" على غوغل يؤدي إلى 1,620,000 نتيجة).

يمتلك التشبيك المحوري للمعلومات ICN مقطع البادئة الأطول بالاضافة الى المحددات التي تسمح لنقل الوسائط، وتسهيلات تم توقعها في قسم الاستعلام من مواصفات بروتوكول DNS الأصلي، ولكن لم يتم تطويرها.

على أي حال، وعلى افتراض أن بوسع المرء جعل حزم 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.

وفي الختام، يمكن للمرء تصور مخطط استبدال DNS بسجل أسم نطاق الشبكة NDN، وعلى الأرجح سيبدأ كمجموعة فرعية من تسهيلات DNS في مرحلة انتقالية قد تستغرق سنوات أو عقود لكي تكتمل. أية محاولات لتعزيز بنية DNS ينبغي أن تستعين وبحرية من برنامج شبكة البيانات المسماة (NDN, Named Data Networking).

إن الشبكة المحورية للمعلومات ICN هي النموذج الوحيد للمستقبل وهو النموذج الأكثر تطوراً. وترى اللجنة بأنه من المفيد دائماً محاولة الخروج بفكرة المبادئ الأساسية ومن ثم دراسة التركيب. [غودسي 2011] هو مثال جيد على طريقة نقله ثالوث الاسم وهوية العالم الحقيقي والبنية التحتية الرئيسية العامة (PKI).

ومؤخراً جداً، أصبح التشديد على توزيع السيطرة[مجلة النيويوركير 2014] والخصوصية التي ظهرت على الساحة مع نظام Namecoin، من الأمثلة الأكثر شهرةً. إن البنية التحية الأساسية العامة الموجودة الآن تمثل المراقبة الواسعة النطاق وهي بمثابة مشكلة فيما يخص الخصوصية. وقد يكون مزيج من العناصر ذاتية الاعتماد وPKI اختيارية أو ربما PKIs متوازية وأنظمة الند للند (P2P) هو الحل. لم يستشكف عمل لجنة ITI هذه المسألة، إلا إنه وجدها أمراً مثيراً للإهتمام.

4. مشاكل التشغيل

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

4.1. تقوية الجذر

نظراً للأهمية المحورية للبنية التحتية للجذر، تم تقديم عدة اقتراحات خارجية للجنة بأن تنظر في تقنيات الحوسبة الموثوقة. ووجدت اللجنة أنه قد يكون ثمة جدوى من هذا النوع من التقنية في الأنظمة المستخدمة لتحوير وتوقيع الجذر، ولكنها وجدت أن النظر بتحسين توزيع البيانات الموقعة على أجهزة المجتمع سيكون بمثابة 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. النسخ المماثلة

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

على سبيل المثال، تنشأ ICANN منطقة الجذر بالشراكة مع Verisign ووزارة التجارة الأمريكية، ثم يتم توزيعها على جميع خواد الجذر من خلال انتقالات المناطق. وبالتالي، فإن ذلك التوزيع، مثل توزيع أية منطقة أخرى في DNS، يمكن أن يتم عن طريق أي آلية: شرائط مغناطيسية وتوصيلات شحنات 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

نشر النسخ عن طريق إشعار DNS أوسحبها عن طريق إستراتيجية اقتراع تبحث عن تغييرات ممكنة. يمكن تأمين حماية انتقالات المنطقة عن طريق توقيع معاملة DNS المختصة بـ (TSIG) و/ أو أي عدد من بروتوكولات النقل، مثل أمن بروتوكول أمن (IPSEC)، وبروتوكول نقل هايبرتيكست ترانسفير (HTTPS).. والخ. هناك مئات الحالات من خوادم الجذر مع نسخ منطقة الجذر.

عندما يريد المستخدمون الوصل الى بيانات في منطقة ملف الجذر يقومون بإرسال أستعلام الى منطقة الجذر. يتم توجيه الاستعلامات بواسطة آليتين: أولهما هي عنوان وجهة عنوان بروتوكول الإنترنت في الاستعلام التي تحدد مجموعة من خوادم الجذر التي تشترك بعنوان شائع لشبكة Anycast، وثانيهما هي أن يقرر نظام التوجيه أي الخوادم في مجموعة Anycast الذي سيستلم الاستعلام. هذا المخطط هو نتيجة لتطور بدأ مع 3 خوادم للجذر ذات عناوين بث موحدة، ثم أتسعت إلى 13 منظومة لخادم الجذر مع تجمعات متشاركة بالحمولة، ثم المخطط الحالي (مع العديد من الخطوات الأصغر فيما بين المراحل). وبكل بساطة فإن "13 خادم جذر" هي في الواقع "13 منظومة خادم جذر" التي تسلم في النهاية ملف المنطقة إلى مئات أو آلاف الخوادم الفردية[1]. سبب وجود 13 منظومة فقط لخادم الجذر، واستخدام أنيكاست، هو أن ذلك أسهل بكثير من تخفيف القيود المفروضة على حجم حزم بروتوكول(UDP) لمستخدمي DNS. كما أن ثمة عدة مشكلات حجم مرتبطة بإضافة عناوين بروتوكل الإنترنت- الأصدار السادس IPv6. على المسار من خادم الجذر إلى المستخدم، يمكن توفير الأمن عن طريق DNSSEC بشكل اختياري.

وعلى مدى السنوات، تعرضت خوادم الجذر الى عدة هجمات والتي معظمها كانت بخصوص مختلف خدمات الرفض الموزعة (DDOS). ومثل هكذا هجمة ولكن تكون ناجحة بإتجاه مستخدم إنترنت معين، ينبغي لها أن تقوم بتشويش الإستفسارات المرسلة الى كافة عناوين Anycast لـ 13 منظومة خادم جذر مختلفة. إن تشويش المجموعات الفرعية يعمل على إبطاء الأداء في الوقت الذي يحاول مرسل الأستفسار أي من خوادم الجذر يجب تجنبها. يمكن أن يكون التشويش إما بإيقاف الخادم أو تعطيل مسار الشبكة إلى الخادم، ويكون عادةً محملاً فوق العادة. لذا وعلى سبيل المثال ففي مثل هكذا هجمات، ظن المستخدمون في كاليفورنيا أن ملف خادم الجذر في ستوكهولم قد تعطل، في حين أن المستخدمون في ستوكهولم لاحظوا العكس. كان رد منظومات خادم الجذر على التهديد الأخير من قبل المنظومة المجهولة من متسللي الإنترنت (hacker) هو نشر المزيد من الحزمة العريضة والخوادم والإشارات الصوتية.

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

لقد كانت بمثابة ممارسة من قبل بعض أعضاء اللجنة تقديم توصية إلى الشركات التي قامت بتشويش نسخ من الجذر داخلياً، وأية مناطق حيوية أخرى، حتى يستمر التشغيل العادي في DNS خلال فترة الهجمة. تعمل ICANN على تسهيل حصول أية منظمة على نسخة من خادم الجذر، ومع المزيد من العمل لتصبح حالة لخادم جذر في منظومة خادم جذر ICANN. كما أنها لفكرة جيدة أن تكون الشركة مكتفية ذاتياً فيما يتعلق بـنظام DNS، وعدم تعرضها للتهديد بسبب انعدام الوصول إلى الخوادم الخارجية، أو بسبب إجراءات من سجل أو أمين سجل أو مشغلي خوادم الجذر أو ما إلى ذلك، سواء كان بالخطأ أو بشكل مقصود.

نظراً لـDNSSEC ، لدينا وسيلة لتوزيع ملف منطقة ما يمكن التحقق منها باستخدام التواقيع الرقمية المغروسة. تعتقد اللجنة بانه يمكن توسيع المبدأ بصوة أكثر عن طريق حماية التفويض والبيانات المعلقة، على سبيل المثال. وقد يكون من الممكن أيضاً القضاء على أو الحد من منظومات خادم الجذر وبيانات العنوان. إحدى المخططات، مبينة بالتفصيل في مساهمة أحد أعضاء اللجنة السيد بول ڤيكسي، وقد تم تضمينها في قسم المساهمات من هذا التقرير.

وثمة جوانب سياسية مهمة أيضاً. فثمة 13 منظومة خادم جذر، وترى العديد من الدول بأنها معزولة ومتأخرة في هذا المجال حتى لو حظيت بالعدد الذي ترغب بتركيبه من خوادم جذر ICANN في بلادهم.
(ناهيك عن ذكر العديد من منظومات خادم الجذر الأخرى الراغبة بتوسيع أبراج Anycast الخاصة بها). إذن فلنترك مناقشة هذه المسألة.

وينبغي التنويه أنه ليس ثمة حاجة تقنية لاستبدال نظام خادم الجذر الحالي لأولئك الذين يفضلونه، لنجعل إستنتاخ ملف الجذر أكثر سهولةً، وكذلك نجعل منه إنموذجاً لملفات المناطق الأخرى.

[1] اليوم، إثنين من منظمات خادم الجذر يتم تشغيلها من قبل نفس المؤسسة وهي Verisign.

4.3. السيطرة على المنطقة المشتركة

ناقشنا في القسم السابق الآراء السياسية التي تجعل الدول راغبة بامتلاك منظومة خادم جذر. قد تكون هذه المخاوف صحيحة أو غير صحيحة، ولكن لاشك بأن تشغيل ملف الجذر الحالي مقره في الولايات المتحدة ويخضع لصلاحيتها القضائية.

وبعبارة بسيطة، يتم تحديث ملف الجذر وفق هذا الترتيب:

- تلقى ICANN طلبات التحديث من TLDs، وتدقق بها بحثاً عن أخطاء
- تقوم ICANN بتقديم التغييرات إلى وزارة التجارة
- تقوم ICANN بإرسال التغييرات الموافق عليها إلى Verisign
- تقوم Verisign بإنشاء ملف جذر موقّع عليه ومن ثم تقوم بتوزيعه

هل هناك طريقة تقنية للتفكير بالتشارك بالسيطرة على ملف الجذر؟ قد تقدمت بعض النظريات. إحدى المدارس الفكرية هي أن البيانات ينبغي أن تحمل س من التواقيع المتعددة. ثم س/ ص، التواقيع هي شروط التحقق من صحة البيانات. وبالطبع، هناك ثمة جدل حول س وص، وما إذا كان التشفير المختلف هو ضروري أو مرغوب به.

لا نهدف هنا إلى الدفاع عن نظام معين، ولكن اللجنة ترى أن التصميم الجيد قد يسمح للعملية السياسية باتخاذ قرار حول كيف ينبغي لسيطرة ملف منطقة معينة أن تتم مشاركتها للبدء بها . رؤيتنا هي إنشاء صندوق أدوات للسيطرة المشتركة على ملف منطقة، وليس للجذر فقط، بل لمشكلات تنسيق خاصة بمنطقة أخرى.
تشير اللجنة الى أن لمجموعة عمل عمليات DNS (أو DNSOPS) ضمن فريق عمل هندسة الإنترنت IETF مشروعين مقترحين لتنسيق معلومات توقيع DNSSEC، ولكنها تتساءل ما إذا كان من الأفضل إنشاء مرافق عامة بدلاً من إيجاد حل لمشكلة هذه النقطة. قد يكون تنسيق العناوين المرسلة والمعكوسة تطبيقاً آخر.

مالمطلوب إذن؟ إننا نخمن بأن النموذج المناسب الذي تتشارك به جميع الأطراف في السيطرة يتمتع بمجموعة من القدرات:

- يتألف نظام الشروع بملف منطقة مشتركة من المنطقة نفسها والقوانين ومساحة منفردة لكل من المشاركين لكي ينشروا طلباتهم وإجراءاتهم
- أجراء أختبارات تقنية أوتوماتيكية لكل منطقة معينة كلما كان ذلك مناسباً
- كل نوع من الطلبات هو مرئي لجميع المشاركين الآخرين الذين يمكنهم اعتمادها أو عدم اعتمادها أو إعادة توقيتها
- قوانين تحدد ما يحدث للطلب
  - أحد القوانين هو التصويت الذي يحدد شروط نجاح الطلب. وقد يشمل هذا تأخير لكل الأطراف لتحظى بالوقت الكافي للنظر في الطلب.
    - بالنسبة إلى ccTLDs، ستملي قوانين مؤتمر القمة العالمي لمجتمع المعلومات WSIS واحدا من س، حتى يتمكن كل نطاق مستوى أعلى لرمز الدولة (ccTLD) من تغيير بياناته الخاصة به.
    - يمكن لنطاقات أخرى استخدام أغلبية بسيطة
  - قد تكون تأخيرات محددة هامة حتى يتمكن الآخرون من الإشارة إلى المسائل التشغيلية والسماح للمتقدمين بالطلبات بإعادة النظر
  - قد تنطبق شروط مختلفة على العمليات المختلفة، مثل إنشاء الجديد مقابل التعديل، وما إلى ذلك.

ثم يمكن لكل مشارك عندها القيام بخوارزمية معيارية لخلق حالة إتساق. قد يبدو هذا خيالاً، ولكن الخوارزميات البيزنطية مثل بيتكوين [آندريسين 2014] ونيميكوين تثبتان أن مثل هذه الأنظمة، ممكنة اليوم.

(يرجى الملاحظة بأن اللجنة لاتقون بإقتراح القوانين، بل مجرد نظام توزيع لتنفيذ أية قوانين يرغب بها المجتمع).

4.4. عمليات السجل/ أمين السجل

جادل بعض أعضاء اللجنة بأنه ينبغي أن توفر عمليات ICANN ضمانات مستوى خدمة، ولكن اللجنة لم ترى بإن ذلك يمثل مشكلة ممكن أن تتفاقم.

4.5. ماهي البيانات التي يتعيّن على ICANN نشرها؟

4.5.1.معلمات ICANN

تدير ICANN العديد من مجموعات المعلمات كجزء من وظائف هيئة أرقام الإنترنت المُخصصة (IANA)، بالإضافة إلى عملية TLD الجديدة، وغير ذلك، مثل العلامت المعكوسة في عدة لغات. وينبغي توفير كل ذلك عبر الإنترنت، ربما في DNS، وبشكل آمن بالتأكيد، حتى يتم استخدامها مباشرة من قبل أي شخص في مجتمع الإنترنت أستخدمت مشروعات أخرى نظام DNS كقوائم عناوين السجل والأنظمة المستقلة ذاتياً وهكذا.

4.5.2.تواريخ ميلاد (إنشاء) النطاق والأنشطة ومجالات أختصاصها

إن سمعة وصورة DNS هي أداة حماية قيّمة. ربما يكون تاريخ إنشاء نطاق ما اليوم، هو جزء المعلومات الفردية الأكثر دلالة من صورة النطاق. ومثل ذلك هو معدل تحديث النطاق لأسماء وعناوين الخادم. وأيضاً فإنه أحياناً يكون من المهم معرفة أي أمين سجل تم أستخدامه لإنشاء وإدارة أسم النطاق. تعتبر النطاقات ونشاط التحديث العالي وبعض أمناء السجلات مثيرة للشك. سيكون من المرغوب توفير هذه المعلومات في الوقت الفعلي، على نطاق واسع.

نوقشت معلومات مجال الأختصاص بطريقة مماثلة ولكنها ستُناقش من قبل IETF في أجتماعهم القادم في لندن في شهر آذار 2014.

4.5.3.نموذج بروتوكول فصل المعرّف ومحدّد المواقع LISP

في وقت مبكر، طلب من اللجنة النظر بإمكانية قيام ICANN بدعم خدمة جذر فائق لبروتوكول فصل المعرّف ومحدد المواقع (LISP)[RFC 6830]. كما تم شرحه لنا من قبل دينور فيريناتشي وآخرين، ستقوم ICANN بتشغيل خوادم LISP كخدمة تجريبية لإحالة الطلبات إلى خوادم LISP الحالية التي لا توفر حالياً اتصالاً عالمياً. لقد حددت ICANN موارد لأربعة خوادم، ولكن المشروع لم يبدأ ا بسبب بعض القضايا العالقة:

- ما هو نطاق (المدة وما إلى ذلك) التجربة؟ ما هي معايير النجاح؟
- ما هي البرمجيات التي ستستخدم ومن سيدعمها؟ كان بديلي الملكية متوفرين.
- من ستكون له السيطرة السياسية والتشغيلية؟
- هل يتعين على ICANN القيام بشئ كهذا أم أمناء سجلات الإنترنت الإقليميين؟
- هل سيتغير الجواب إلم يتم إنخراط عناوين بروتوكول الإنترنت؟

لم يتم إتخاذ أي إجراء حول هذه التجربة.

شعر بعض أعضاء اللجنة أن بروتوكول "LISP هو مجرد مثال واحد على درجة أكثر عموميةً لتقنيات توجيه النقل، وبالتالي، لم تمثل أية مهمات لإدارة معرّف مبتكرة تقع خارج ممارسات إدارة المعرّف التشغيلي الحالي، وبالتالي، فإن الحالة التي تتطلبها طريقة التوجيه المحددة هذه تتطلب إنتباه ودعم خاص من ICANN لم تكن مؤكدة بوضوح".

ينبغي على ICANN أن تتوقع ورود أسئلة بخصوص السياسة والقضايا التقنية حول المعرّفات الجديد وأن تقوم بالتخطيط وفقاً لذلك.

4.6. التضاربات (تضارب الأسماء)

لقد كان معظم أعضاء اللجنة على دراية بمشكلة تضارب أسماء نظام DNS، وبينما كان هناك الكثير من النقاشات حول هذه المشكلة، إلا إنه لم تنبثق أية توجيهات جوهرية جديدة. ولقد رأت اللجنة أن توصي بتبنّي بنماذج العالم الحقيقي للنظام المبين في [ICANN 2013].

5. أسس بروتوكول نظام DNS

هل يمكننا تخيل مراجعة أساسية وتطوير نظام DNS وإحداث قفزة به؟ يرى العديد ومن ضمنهم بعض أعضاء اللجنة بإن القاعدة التي تم تنصيبها مقاومة جداً أو قد تمثل إشكاليةً[2]، أو البدء مجدداً هو فكرة صحيحة.

وبشكل مفاجيء، أجمعت اللجنة على الاعتقاد بأن بذل الجهود لتشخيص هذه المشاكل والبحث عن حلول لهو أمرٌ يستحق العناء، حتى ولو كان ذلك لأجل إيقاف تفاقم المشكلة على الأقل. في هذا القسم تضع اللجنة ملخصاً لبعض المشاكل التي ينبغي أن تُبحث إذا كان يتوجب القيام ببذل جهود أوسع.

لقد كان لتاريخ الابتكار في DNS النجاح والفشل على حد سواء. أحد الدروس الرئيسية هو أنه لا يتم تبني التكنولوجيا بشكل واسع إلا إذا كانت قادرة على توفير فائدة معينة. وحرص الإداريون على أن يُبقوا على مناطقهم مربوطة مع DNS العالمي وعلى تحديث سجلات A وMX أولاً بأول، وإلا سوف لن يحصلوا على أي بريد يصلهم أو أي نشاط في الإنترنت. ولكن من بين حوالي 60 نوع سجل تم تحديدها، فقط أقل من 10 منها تشهد استخداماً واسعاً.

وواجهت الجهود المبذولة لإنشاء تطبيقات مستندة على DNS، مصاعب مماثلة.

وأقترحت مجموعة مبكرة من طلبات التعليقات RFCs الخاصة بنظام DNS طريقة لتوجيه البريد الى صناديق بريد معينة، ولكن لم يتم تنفيذ ذلك أبداً. وقام مخطط ثانٍ (MX RR) بحل مشكلة توفير خوادم البريد الزائد علاوةً على توفير توجيه البريد خلال الحدود التنظيمية - وهي أسس توجيه البريد حالياً. تم تبني قواعد بيانات مضادة للبريد غير المرغوب به بشكل واسع من دون تحديد معايير. أدت جهود المعايير المتضاربة للتحقق من صحة البريد إلى تنفيذ مبادرتني اثنين باستخدام TXT RRs، وجدل حول ما إذا كان وضع معايير أنواع جديدة سيكون مفيداً.

لقد كان لجهود خطة ترقيم E.164 NUMber أو مايرمز لها بالرمز (ENUM) لتعيير توجيه الهاتف ووسائل الإتصال باستخدام نظام DNS، أيضاً النجاح المحدود. ورغم اعتبار تكنولوجيا مؤشر هيئة الأسماء (NAPTR, Name Authority Pointer) على أنها ابتكار حقيقي، إلا إن مصممو ENUM تجاهلوا الحاجة إلى توجيه معلومات غير رقم هاتف الوجهة، وفضل مصنّعو المعدات الحفاظ على القيمة في أنظمة الملكية الخاصة بهم.

5.1. المبادئ الإجمالية

ينبغي على كل تصميم جديد أن:

- إزالة تحديدات الحجم- من الأرجح أن 576 بايت هي وحدة النقل القصوى (MTU) قد ساعدت على تأخير DNS أكثر من أي عامل فردي آخر؛ وإن DNSSEC لا تتناسب آليات التمديد لنظام DNS على الرغم من ذلك، وعليه فالعديد من البرامجيات والاجهزة سوف لن تسمح بمرور الحزم الكبيرة.
- الحفاظ على الإتصال مع كافة أسماء نظام DNS المتواجدة والبيانات.

[2] تتغير الأفكار هنا. يقول البعض بأن عملية IETF كانت "مجزّأة" في مجاميع عمل محددة (خصوصاً في الماضي). ويرى آخرون بإن واجهات معالجة الطلب (APIs) ضرورية جداً وإن فريق عمل هندسة الإنترنت لايمتلك هذه الواجهات، ولكن من يمتلكها؟ ويظن البعض بإن مجاميع عمل DNS المتنوعة تعمل على تعجيل التطور والأبتكار بصورة أفضل مما قد تقوم به رؤية إجمالية.

- يحاول تعزيز التنفيذ المتسق للأنظمة - فإلم يتبع المنفذون المختلفون المواصفات الموضوعة، فإن مستخدم الإنترنت سوف يواجه تحديدات تجاه أي تداخلات مشتركة قد تحصل.
- يسمح لتوسع مستقبلي
- توفير حوافز للإعتماد

5.2. نموذج البيانات

تصورت DNS RFCs مساحات اسم متوازية "الطبقات" مختلفة من المعلومات، وأنواع البيانات الجديدة التي تتألف من مكونات بسيطة. لم يتم استكشاف مفهوم 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 العلامات كوكيل عن نوع RR.

ستجادل اللجنة بأنه إما ينبغي على DNS تعريف أنواع RR الخاصة بها والتنسيقات في البيانات حول البيانات المنقولة في DNS، أو ينبغي على DNS أن يقوم بصياغة العلامات الصغيرة على أنها آخر نوع من البيانات وتوسيع الاستعلام للسماح بالمزيد من المطابقة المرنة.

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 المصدر "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 والتي قد تنعش مجموعات البيانات المخزونة من دون نقل البيانات فعلياً.

كما تعتقد اللجنة أيضاً بأنه يمكن تحسين الأمن عن طريق المزيد من الاستنساخ المتكرر للمناطق (الأصغر)، بإستخدام إنتقال المنطقة الحالي وكافة الآليات. لا تحتاج هذه البيانات إلى الحماية من DNSSEC، وبالتالي، يمكن تحسين الأمن في المناطق التي لا يتم تنفيذ DNSSEC بها.

5.4. برنامج واجهة برنامج التطبيق (API)

ثمة شكلين اثنين لـواجهة برنامج التطبيق API لنظام DNS: 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.

إن برمجة API قد مرت خلال عدة محاولات للمراجعة وقد فشل معظمها. ومؤخراً، شاهدت اللجنة عرضاً من قبل بول هوفمان حول التصميم الجديد الذي يظهر الواجهات غير المتزامنة ودعم DNSSEC. وتم عرض العمل أخيراً من قبل فريق عمل هندسة الإنترنت IETF في لندن في شهر آذار 2014. شاهد http://vpnc.org/getdns-api/

ولكن بغض النظر عن API، ثمة سؤال بخصوص أي ينبغي إجراء 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 أو خادم في بيئة المستخدم وما إلى ذلك، وبحسب ما يفضل 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 أي 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.

5.5. بروتوكول الأستعلام

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

تبدأ مشاكل نقل بروتوكول مخطط بيانات المستخدم UDP الأصلي مع تحديدات وحدات النقل القصوى 576 بايت التقليدية. كان التصليح الأصلي يعني الرجوع الى بروتوكول السيطرة على الأنتقال لأجل تحقيق إنتقال أكبر. ربما كان حجم بيانات الجذر هو أول مكان أحدثت به تحديدات وحدة النقل القصوى MTU تأثيراً واسع النطاق أدى إلى حدود 13 خادم جذر، ثم لاحقاً إضافة توقيعات DNSSEC الجذرية ساعدت كثيراً على توسيع حزم الرد. تم التفكير بـ EDNS0 لحل هذه المشكلة، بالإضافة إلى أمور أخرى، وقد أستطاعت أن تحقق بعض النجاح. ولكن هناك ثمة تحديدات أخرى مثل مختلف أحجام إطار بروتوكول Ethernet.

وكذلك لايستطيع EDNS0 حل مشكلة نقاط الولوج، والموجّهات وحواجز الجدران النارية firewalls والأجهزة الأخرى التي تحجب الولوج الى منفذ 53 لبروتوكول السيطرة على الأنتقال TCP، أو تحديد حجم الحزمة أو حتى إعتراض طللبات DNS بتفويضات شفافة غالباً ماتكون على حساب الخدمة. قد توجد مشاكل مماثلة في تخزين خوادم الأسم والتي لاتدعم الحزم الكبيرة، وكافة أنواع بيانات نظام DNS و EDNS0 ... الخ. بعض المشاكل قد تكون دقيقة جداً. في أحد الأمثلة، تمر حزم DNSSEC عادةً ولكن ليس أثناء الإنقلاب الرئيسي لـDNSSEC ، وهي عملية صيانة اعتيادية، حيث تكون الحزم أكبر قليلاً.

إحدى المشكلات المرتبطة هي هجمات DNS DDOS، وخاصة باستخدام الانعكاس والتضخيم. في تلك الحالات، سترغب بطريقة لتحديد حركة المرور المشروعة من حركة الهجمات. سيحل التحقق من صحة العناوين جزءاً كبيراً من المشكلة، لـكل من DNS وللعديد من البروتوكولات الأخرى على حد سواء. تدعم اللجنة ذلك[3]إلا إنه لم يتم نشره بشكل واسع. يمكن أن يساعد معدل التشكيل ومختلف أنواع الوسائل التجريبية، ولكنها ليست بالحلول الحاسمة. كانت ولاتزال آليات التحقيق الخفيفة المتنوعة وستبقى حلولاً محتملة.

تدعو إحدى المدارس الفكرية بخصوص حل مشكلة النقل بوضع كافة تحرك 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. وتشمل البدائل بروتوكول معاملة جديدة أو وسيلة لاستخدام UDP، وكلاهما قد لا يعملان في أجزاء من القاعدة المنصّبة. في كلتا الحالتين، ثمة مسألة ما إذا كانت معاملات DNS تستخدم شكلاً تقليدياً أو جديداً.

بغض النظر عن النقل، ينبغي توسيع بروتوكول استعلام DNS للسماح بالمزيد من الاستعلامات المرنة. وقد تشمل هذه نوعاً من التحكم بالولوج إلى العلامات الوريثة بدلاً من NSEC وNSEC3.

تعلمت بروتوكولات عالم الأبحاث مثل CCN من DNS ودمجت جميع هذه المميزات. مشكلة هذه البروتوكولات الجديدة هي أكبر من تحديد كيفية تحفيز ترقية للبنية التحتية الحالية مع بعض التوافق الرجعي، بدلاً من تحقيق انفراج جديد في علم البروتوكول

6. الملاحظات والتوصيات

- سيتسمر نمو إستخدام DNS في البنى التحتية؛ وقد جوبِهَ إستخدام DNS في واجهة المستخدم (UI) من قبل البدائل القائمة على البحث وواجهات الهواتف النقّالة ..الخ.
- يتعيّن على ICANN نشر المزيد من بيانات DNSSEC الموقعة للأسماء المحفوظة..ألخ.
- بالتعاون مع فريق عمل هندسة الانترنت والجميع، قم بإجراء دراسة لتحديد الرؤية الأنشائية لنظام أسم النطاق DNS في عام 2020.
- لتصميم نموذج Prorotype لجذر مفتوح.
- تصميم ملف نظام سيطرة مشترك للجذر.
- أداء تمارين تضارب للأسماء لإختبار سهولة التنفيذ [ICANN2013].

[3] يدعم كافة أعضاء اللجنة بروتوكول [BCP 38] المثالي ويرى بعض أعضاء اللجنة إن دعمهم له ينبغي أن يكون ضمن واحدة من توصيات اللجنة الأساسية. وبكل الأحوال، يرى الغالبية بإنه كان هناك إعتماد قليل منذ نشر بروتوكول BCP في عام 2000.

7. المصادر

"Why Bitcoin Matters" Andressen [Andreesen 2014]
http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters

[BCP 38] فلترة دخول الإنترنت Ferguson el al, “Network Ingress Filtering: القضاء على هجمات رفض الخدمة التي تستخدم إنتحال عنوان مصدر بروتوكول الإنترنت" RFC 2827 أيار 2000.

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

[فياض بقش 2013] فياض بقش وآخرون، " Less Pain, Most of the Gain" : القابل للنشر تدريجياً ICN سيغكوم 2013

[غودسي 2011] غودسي وآخرين، "Naming in Content-oriented Architecture"، سيغكوم 2011

[هاستون 2013] دراسة DNS عبر TCP فقط.

/http://www.circleid.com/posts/20130820_a_question_of_dns_protocols
and the ensuing thread on dns-operations

[[ICANN 2013] "دليل تحديد تضارب الأسماء والتخفيف منه للمختصين في مجال IT" (Guide to Name Collision (Identification and Mitigation for IT Professionals
https://www.icann.org/en/about/staff/security/ssr/name-collision-mitigation-05dec13-en.pdf

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

[الجدارة] الأقسام حول النطاقات ونظام DNS

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"،88 SIGOMM

[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، "جدول وخطة 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

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

8. قاموس المصطلحات

A سجل من نوع نظام DNS يستخدم لحمل عنوان IPv4

AAAA سجل من نوع نظام DNS يستخدم لحمل عنوان IPv6 ويطلق عليه تسمية "quad A"

AI (الذكاء الصناعي) Artificial Intelligence

API واجهة برنامج التطبيق Application Program Interface

BCP (أفضل ممارسة حالية) (Best Current Practice) مجموعة فرعية محددة من طلبات التعليقات ROC

CCN التشبيك المحوري للمحتوى Current Centric Networking

ccTLD نطاق المستوى الأعلى لرموز البلدان - وهو نطاق مستوى أعلى تم تفويضه لبلد معين ويتم تشغيله من قبل طرف ثالث

DANE التحقق من صحة الكيانات المسماة بحسب DNS (DNS-based Authentication of Named Entities)

DDOS الرفض الموزّع للخدمة

DNS نظام أسم النطاق - نظام تسمية الإنترنت

DNSOP DNS Operations - مجموعة عمل من فريق عمل هندسة الإنترنت IETF مهتمة بمشاكل عمليات DNS وغيرها.

DNSSEC الإمتدادات الأمنية لنظام إسم النطاق

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 DNS [RFC 2671] – 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 مؤسسة فيديكس للبريد السريع Federal Express

FQDN إسم النطاق المؤهل كلياً Fully Qualified Domain Name

ETP بروتوكول نقل الملفات File Transfer Protocol

gTLD نطاق المستوى الأعلى العام Generic Top Level Domain وهو النطاق الذي لاصله له برمز البلد

HTTPS مصدر بروتوكول نقل النص التشعبي الآمن

IANA هيئة الإنترنت للأرقام المخصصة Internet Assigned Number Authority

ICANN شركة الإنترنت للأسماء والأرقام المخصصة Internet Corporation for Assigned Names and Numbers

ICN التشبيك المحوري للمحتوى (Information Centric Networking)

IEEE معهد مهندسي الكهرباء والتقنية الإلكترونية Institute of Electrical and Electronics Engineers

IETF فريق عمل هندسة الإنترنت Internet Engineering Task Force

IOT إنترنت الأشياء Internet of Things

IP بروتوكول الإنترنت Internet Protocol

IPSEC أمن بروتوكول الإنترنت Internet Protocol Security

IPv4 روتوكول الإنترنت الإصدار 4

IPv6 بروتوكول الإنترنت الإصدار 6

ITI إبتكار تقنية المعرّف (Identifier Technology Innovation) - وهو أسم لجنة إستراتيجية لدى ICANN

LISP بروتوكول فصل محدد الموقع والمعرّف [Locator/Identifier Separation Protocol RFC 6830]

قاعدة معلومات الإدارة MIB

MTU وحدة النقل القصوى Maximum Transmission Unit- وهو الحجم الأقصيى للبيانات التي تستطيع المرور بدون أية تجزئة

MX تبادل البريد (Mail Exchange) - من نوع بيانات DNS التي تحدد تبادل البريد الذي يتعامل مع رسائل من نطاق معين

NAPTR مؤشر هيئة الأسماء- نوع بيانات DNS يستخدم بشكل واسع في الإرسال الهاتفي للإنترنت (Name Authority PointTer)

NDN تشبيك البيانات المسماة Named Data Networking

P2P الند للند (القرين للقرين) Peer to Peer

PKI البنية التحتية الأساسية العامة Public Key Infrastructure

RFC طلب التعليقات (Request for Comments) - مذكرات توثق مشاكل الإنترنت التقنية والتشغيلية

RIR سجل الإنترنت الإقليمي (Regional Internet Registry) واحدة من التنظيمات التي تتعامل مع تخصيص تسجيل مصادر أرقام الإنترنت ضمن منطقة معينة في العالم. على سبيل المثال ، ARIN، السجل الأمريكي لأرقام الإنترنت الذي 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 المورد- الوحدة الذرية للمعلومات في نظام DNS.

TSIG توقيع المعاملة Transaction Signature

TTL وقت الأستمرار Time to Live

TXT نوع سجل الموارد النصي في DNS الذي يتيح الحقول النصية ذات التنسيق الحر

UDP بروتوكول مخطط بيانات المستخدم User Datagram Protocol - بروتوكول مخطط بيانات الإنترنت بدون إتصال

UI واجهة المستخدم User Interface

URL المعرف الموحد لمصدر المعلومات

URI محدد مواقع ويب الموحد لمصدر المعلومات

WIFI الدقة اللاسلكية Wireless Fidelity- معايير الشبكة اللاسلكية المحددة من مجموعة معايير IEEE 802.11

9. مساهمات أعضاء اللجنة

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

9.1. المساهمة المقدمة من قبل جيمس سينغ

البنية التقنية

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

لذا فإن تقنية مثل تقنية نيميكوينس (namecoins) أو نظام المعرفات اللا مركزية الآخر تثير اهتمامي.

ولكن ليس ثمة نظام معرفات لا مركزي ولكن ما أعرفه هو نظام معرّف والذي أستخدمه بصورة واسعة. لذا سواء أعجبكم هذا أم لا، ما زال نظام DNS هو أحد الأنظمة المعرّفه المنتشرة التي بحوزتنا. وكما نفعل في IETF، إن"الرموز العاملة" هي التي تفوز وليست بالضرورة أن تكون الأفضل.

أنا لا أؤمن بتعدد الجذور أو الجذر البديل. وكما قلت في بوينس آيريس، أنا أؤيد RFC 2826. الجذر المتعدد والجذر البديل وكل مقترح ذو صله يقوم بنقل المشكلة السياسية إلى طبقة أخرى فقط، ولكنها لا تحل المشكلة السياسية الأساسية. لاحظوا أنني قلت مشكلة سياسية لأنني لا أعتقد أن الجذر المتعدد يحل أية مشكلة تقنية على الإطلاق، بل إنها في الحقيقة تزيد من التعقيد التقني.

ICANN

أدى نظام DNS وطبيعته المركزية للجذر وبشكل جزئي في جعل تشغيل وظيفة IANA البسيطة الأصلية ينتج عنه منظمة كبرى يطلق عليها اليوم إسم ICANN.

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

ولكن ICANN هي "الرمز العامل" لتنسيق معرّفات DNS. ربما ثمة تصاميم أفضل، وربما تكون أبسط وأكثر أناقة (وكما يرغب العديد من أعضاء مجتمع IETF بإن يمكننا الرجوع إلى أيام جون بوستيل)، ولكن هذا هو الحال اليوم، والأهم من ذلك، فإنه ناجح رغم أنه يمكن أن يصبح أفضل. إن لإتحاد الأتصالات الدولي (ITU) المقترح البديل الذي نعرفه مشاكل أخرى أو ربما المشاكل الأسوء.

لذا أنا أؤيد ICANN لأنه أفضل نظام ناجح لدينا لتنسيق معرفات DNS و ملف الجذر.

تمديد DNS ونظامه إلى مجالات أخرى

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

أؤيد وأرغب برؤية النظام البيئي لِـ DNS (الذي يشمل معايير DNS، عمليات الجذر، ICANN.... الخ) الذي لدينا الآن والذي تم تصميمه بالأصل لـ DNS وأن يتطور ليمتد إلى مناطق أخرى (مثل RFID، وبذلك يتمكن ضم المزيد من المجتمع. العمل الذي قمنا به بخصوص أسم النطاق المدوّل IDN يضم مجموعة من المستخدمين في المجتمع الذين يحتاجون إلى استخدام لغتهم الأصلية الخاصة في النظام البيئي لنظام DNS، بدلاً من السماح لهم بإنشاء نظامهم الخاص بهم.

وبينما جادلني البعض بخصوص فيما لو قمنا بـإنشاء IDN خارج النظام البيئي لنظام DNS ، فإن عملية النشر كان يمكن أن تكون أسرع (مثلاً، راجع الكلمات الرئيسية في اللغة الأصلية)، ويمكنني القول بأن IDN هو أفضل أيضاً لأنه جزء من النظام البيئي لـِ DNS، حيث ثمة معايير مفتوحة معرّفة بصورة جيدة وتطبيقات مفتوحة وشركات من شأنها أن تضيف الى ثروتنا من DNS، وبصورة مشابهة لحماية مشتركي IDN والمستخدمين النهائيين له.

وعلى هذا النحو، لا أشعر بتأنيب الضمير، وأؤيد استكشاف كيف يمكننا توسيع DNS إلى معرّفات لم يتم تصميمه لها بالأصل. غالباً ما يكون المهندسون الذين يصممون المعرّفات غير ملمّين بالسياسات التي ترافق المعرّفات، وخاصة إذا كانت مثل هذه المعرفات مكشوفة أمام المستخدمين النهائيين. يمكنهم معرفة أمر أو أمرين من تاريخ معرّفات DNS في ICANN.

سياسات ملف الجذر

إن سياسات ICANN وكيف ينبثق العديد من وجهات نظر ICANN كجزء من " حوكمة الإنترنت" من دور ICANN في تنسيق خوادم الجذر.

لتزداد الأمور سوءاً، تم تنصيب 11من أصل 13 خادم للجذر في الولايات المتحدة، بسبب مصادفة تاريخية، ولكن هذا يجعل من فكرة وقوع ICANN تحت سيطرة الولايات المتحدة أمراً بالغ السوء، وخاصة في هذه الأيام التي تعقب قضية سنودين.

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

أستطيع أن أقبل "التاريخ" كمبرر.

ولكنني لا أستطيع قبول 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 بوينس آيريس أن بوسعي التفكير ببضعة حلول تقنية، تكفي كهوية على الأقل. لا يمكننا السماح لـ ICANN بمواصلة استخدام IETF/ و المبررات التقنية كعذر للمشكلات السياسية التي تواجهها. ينبغي أن نكون قادرين على إخبار ICANN، بنعم يمكننا القيام بذلك، ولكن القرار السياسي للقيام بذلك أو لا عائد إليكم.

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

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

يدرك معظم المهندسين على الأرجح ما قلته أعلاه، ولكن معظم العاملين في ICANN لن يفهموه.

لذا ثمة اعتبارات عند اختيار مشغل خادم الجذر، لأن هذا يعد أمراً أساسياً لاستقرار معرّفات الإنترنت، ويستند الكثير منه على الثقة. ولكن الثقة ليست مشكلة هندسية، سواء أعجبكم هذا أم لا.

- جيمس سينغ

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

لماذا يعتبر DNSPod مفيداً في الصين رغم طريقة " تقسيمه" لنظام DNS.

9.2. قرار DNS وسلوك تطبيقات قائمة البحث - جيف هاستون

لا يوجد - لم يقم أي أحد بإجراء أي بحث بخصوص DNS

أبداً - بحث إسم القاعدة، ولكن لم يطبق قائمة البحث

قبل - يطبق قائمة البحث، وإن أعاد NXDOMAIN فسيبحث نفس القاعدة

بعد - يبحث أسم القاعدة، وإن أعاد NXDOMAIN فسيطبق قائمة البحث

دائماً - لايبحث بإسم القاعدة- فقط يطبق قائمة البحث

سلوك مكتبة مقرر DNS لنظام التشغيل الأساسي

نظام	مطلق *خادم*	علامة منفردة نسبية *خادم*	متعدد العلامات نسبي *www.server*
MAC OSX 10.9	أبداً	دائماً	أبداً
Windows XP	أبداً	دائماً	بعد
Windows Vista	أبداً	دائماً	أبداً
Windows 7	أبداً	دائماً	أبداً
Windows 8	أبداً	دائماً	أبداً
FreeBSD 9.1	أبداً	قبل	بعد
Ubuntu 13.04	أبداً	قبل	بعد

سلوك المتصفح على منصات MAC و Windows

MAC OSX 10.9

	خادم sever	*خادم server*	*www.server*
Chrome (31.0.1650.39 beta)	أبداً	دائماً	قبل
Opera (12.16)	أبداً	دائماً	أبداً
Firefox (25.0)	بعد*	دائماً	بعد*
Safari (7.0 9537.71)	لا يوجد**	لا يوجد**	لا يوجد**

* إستطالة "www." المضافة، وبعد ذلك محاولة أضافة المقطع "www." أيضاً مرفقاً بقائمة البحث

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

Windows 8.1

	خادم	خادم	*www.server*
Explorer (11.0.900.16384)	لايوجد	لايوجد	أبداً
Firefox (25.0)	أبداً *	دائماً	أبداً
Opera (17.0)	لايوجد	لايوجد	لا يوجد**
Safari (7 7534.57)	أبداً *	دائماً ***	أبداً

* إستطالة "www" مضافة

** OPERA على دراية بنطاقات TLDs المفوضة وتستفسر فقط عن متى يكون الرمز الأخير نطاق من نوع TLD

*** أستطالة "www" و ".com" المضافتين

9.3. ملاحظات حول الأتساق والمساهمة الموجهة – جيوف هيوستن

إن توجب أن النظر الى أصول نظام أسماء النطاقات، فإنه سيتم أيجاد ما يسمى "ملف المستضيف" كمحاولة مبكرة لإضفاء الأستخدام البشري إلى سياق شبكات الكمبيوتر. استخدمت ARPANET نموذج تسمية عقدة شبكة حيث كان لكل عقدة متصلة ملف تكوين محلي، وملف المستضيفين، التي أحتوت على أسماء عقد ARPANET الأخرى، وعناوين البروتوكول لكل عقدة. لم يكن هناك ثمة اتساق منفذ على نطاق هذه الحالات المتعددة من ملف المستضيف هذه، على نطاق مجموعة العقد المتصلة بواسطة ARPANET، ولا كان آنذاك، ثمة وسيلة لتوزيع نسخة عن ملف المستضيف عبر شبكة الإنترنت. كانت خدمة ملف المستضيف هذا هي توفير أسماء ودية للبشر مكان عناوين 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. ومع نمو ARPANET، ازداد أيضاً حجم ونسبة تحديث ملف المستضيف وارتفعت النفقات الأساسية لصيانة مستضيف محلي دقيق أيضاً. تم تحديد معايير صياغة 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. تم الحفاظ على آلية ترجمة الأسم المحدد على أنه سلسلة بشرية ودية إلى عنوان خدمة خاصة بالبروتوكول عن طريق النقل من ملف المستضيف إلى DNS.

ثمة عدد من الخصائص لفضاء المعرّف هذا، ومن بينها الملاحظة بأن DNS يوسع فضاء الأسم المناسب للاستخدام في حوار بشري، وفي الوقت نفسه الاعتراف بهيكل رسمي كافٍ للسماح بالتلاعب بالأسماء بواسطة تطبيقات كمبيوترية بشكل قطعي. إن فضاء أسماء DNS هو فضاء هيكل هرمي يسمح لفضاء الأسم البحث في فضاء الأسماء بفعالية لأجل التطابق التام، وفي الوقت نفسه يسمح لإطار عمل الإدارة الموزعة لأسماء الفضاءات. وطالما يتم تجنب تضارب العلامات ضمن أية منطقة فردية لهرمية أسماء DNS، يمكن تجنب تضارب

الأسماء ضمن كل فضاء أسماء DNS الإجمالي، 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 المصادر المسماة والتي تشير إليها خدمتنا. لقد كان في النية أن يكون DNS متسقاً، من ناحية أنه نظراً لإدخال اسم متسق في DNS، ينبغي أن توفر الاستعلامات حول ذلك الاسم نفس الرد على نطاق مواقع متنوعة من الطرف المستعلم والأوقات المختلفة للاستعلام. يسمح هذا بالاتساق المرجعي، من ناحية أنه يمكن تبادل إسم DNS بين الأطراف والإشارة إلى مصدر متسق من موقع الخدمة. ليس الهدف أن يحل نظام DNS محل نظام دليل أو نظام بحث. إذا كان ثمة مطابقة دقيقة للاسم الذي يتم الاستعلام عنه في DNS، ستكون نتيجة استعلام DNS هي القيمة الموجهة لذلك الاستعلام، وإلا سيعيد الاستعلام فشل في المطابقة.

خضع نموذج فضاء أسماء DNS كفضاء أسماء المعرّفات لدعم الواجهة البشرية مع الشبكة منذ تشغيله للعديد من التغييرات، مبدئياً رداً على نمط الاستخدام البشري للمعرفات في الأتصالات. إننا نميل إلى استخدام المعرّفات بأشكال أقل دقة، وبأشكال تتضمن عناصر من السياق المحلي تستخدم لغات ونصوص محلية، وعلى مرور الوقت، كان دور DNS كشكل من أشكال الواجهة البشرية لمصادر وخدمات الشبكة مندرجاً ضمن جهود دعم الواجهات التي تعمل بشكل أكثر "طبيعيةً" للاستخدام البشري.

اقترح RFC1034 استخدام شكل من أشكال الاختصارات في الكتابة في شروط أسماء DNS، حيث يتم اعتبار الأسماء التي لا تنتهي بتذييل '.' على أنها "أسماء مرتبطة"، وكما هو مثبت في RFC1034، "تظهر أغلب الأسماء المرتبطة على واجهة المستخدم، حيث يتنوع تفسيرها من تطبيق إلى آخر". عادةً، يتضمن مثل هذا التفسير المحلي الجمع بين قائمة البحث المحلية من لواحق العلامة، مما يسمح 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 لفضاء معرّفات 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 لـِ URL وتطبيق تحويل إسم من الإضافة لبداية السلسلة "www." وإضافة لاحقة معرفة محلياً (غالباً ما تكون ".com"). بهذا الشكل، يصبح المعرف الذي حدده المستخدم وإسم المعرّف المستخدم في استعلام DNS اللاحق مرتبطان، ولكن ليسا متشابهين بالضرورة.

تم توسيع هذا الاستخدام لتحويل الاسم المحلي بحيث تم توجيه معرّفات تشكلت من نصوص لغات عدا عن US ASCII إلى DNS (IDNs: RFC 5891). كانت هذه عملية محددة بوضوح حيث يتم تحويل المعرّف الذي أدخله المستخدم إلى سلسلة علامة مشفّرة تشكل إستعلام DNS. في هذه الحالة، يكون التحويل محدداً بدقة، بحيث تهدف التطبيقات المتعددة لمعيار IDN إلى دعم نظرة متسقة لتوجيه معرّف في نص معين إلى شكل اسم DNS مشفر.

وكان ثمه ارتقاء آخر بصقل نموذج التفاعل البشري وهو توحيد مصطلحات البحث وURLs كمدخلات في المتصفحات. في هذه الحالة، إذا لم يستخدم المستخدم المواصفات الكاملة لـ URL الى المتصفحة، سيحاول المتصفح بتأريخها.

9.4. بعض المشاكل المصاحبة لتقنيات المعرّفات الحالية - ريك بويڤي

1. مرونة ملف منطقة الجذر

يعتمد نظام DNS اليوم إعتماداً كبيراً على توفر خوادم الجذر وقدراتها وإمكانية الوصول إليها. إن حافظت مؤسسة أو مزود لخدمة الإنترنت أو بلد أو مستخدم على نسختها (نسخته) من ملف منطقة الجذر وأستخدمت تلك النسخ لحل أسماء النطاق بدلاً من من التوجه دائماً الى خوادم الجذر "الحقيقية"، فإنه من الأفضل لكل من المشار إليهم هنا أن يُعزلوا عن الهجمات على خوادم الجذر وسيكون بإمكان كل منهم الأستمرار بالعمل بصورة طبيعية عندما يتم فصلهم عن خوادم الجذر الحقيقية عندما تصبح ملفات الجذر الحقيقية غير متوفرة، أو محملة بأكثر من طاقتها أو في خطر.

2. الأستخدام الأحتيالي لعناوين بروتوكول الإنترنت IP

إن حزم بروتوكولات الإنترنت IPمع عناوين مصدر مزورة هي واحدة من أهم الأدوات التي يستخدمها المخربون هذه الأيام لمنع أهدافهم من إستخدام الإنترنت. وبإرسال الحزم التي تبدو وكأنها قادمة من المصدر المستهدف من قبل المخرب وحصول هذه الحالة من عدد كبير

من الأجهزة، يستطيع المخرب أن يسبب عدد كبير من "أستجابات" حركة المرور التي ستملأ أو أو تتجاوز في ملأ روابط الإنترنت التي سترجع الى الهدف.

3. رسم مخطط التدفق السريع لأسماء وعناوين نظام DNS

اليوم يتم إنتهاك نظام DNSغالباً من قبل المخربين بطريق تتيح لهم تجنب محاولات الجهات الرسمية لتعقبهم وأبطال أنشطتهم غير القانونية. قد يستخدم برنامج "bonet master" اليوم مجموعة من آلات الخطف ("botnet") لمختلف أنواع الأنشطة غير القانونية بما في ذلك إرسال البريد غير المرغوب فيه (spam) والشروع بهجمات الحرمان الموزع للخدمة (DDoS, Distributed Denial of Service) بضرر لأجهزة أخرى مع مختلف أنواع البرامجيات الضارة. وبالتغير المضطرد الحاصل في رسم مخطط أسماء وعناوين نظام DNS تستطيع برامجيات bonet masters تحريك أنشطته غير القانونية بسرعة من مجموعة واحدة من الأجهزة المتأثرة الى أخرى محاولاً المراوغة والتملص من السلطات الشرعية لتعقبها وإبطال إنشطتها غير القانونية.

نحن نوصي بأن تعمل ICANN مع الآخرين من مجتمع الأنترنت:

(1) لتحسين مرونة ملف منطقة الجذر،

(2) لمعالجة الأستخدام الإحتيالي لعناوين بروتوكول الإنترنت IP

(3) لمعالجة مشكلة التدفق السريع لرسم مخططات أسماء وعناوين نظام DNS.

9.5. الشبكة الدولية لملف منطقة الجذر - پول فيكسي

نظرة عامة:

نحن نقترح بإن تقوم IANA بإنتاج عدة أشكال إضافية لملف منطقة جذر نظام DNS للسماح لشبكة Anycast العالمية والبحث التشغيلي. " Anycast الدولية" تعني في هذا السياق ملف لمنطقة الجذر الذي تقوم سجلات apec NS الخاصة به بإدراج خادمين للأسم فقط والتي عناوينها المعروفة بـ (سجلات A و AAAA) والتي يمكن إستضافتها من قبل أي أحد. يتضمن "البحث التشغيلي" في هذا السياق إختبار على نطاق واسع لخدمة أسم جذر IPv6 فقط وأختبارات عامة على نطاق واسع لآثار تضارب أسماء نطاقات "new gTLD". يعامل هذا المنهج خدمة أسم الجذر كموقع خدمات غير مدار بدلاً من كونه خاضع لإدارة.

معلومات أساسية وخلفية

لايمكن تشغيل شبكة Anycast الدولية لملف منطقة الجذر بصورة آمنة ومسؤولة قبل توفر DNSSEC لأنه بدون DNSSEC سيكون من الممكن تكوين الخادم المجيب بصورة إجبارية من بيانات ملف جذر نظام DNS بما في ذلك نطاقات المستوى الاعلى TLDs أو نطاقات TLDs المعاد تفويضها. الآن مع DNSSEC أصبح من الممكن لمشغلي خادم الأسم المسترجع لإكمال تشغيل DNSSEC وبهذا لابد من إستحصال موافقة IANA على أية معلومات خاصة بنطاق gTLD يسمع بها من خادم أسم جذر شبكة Anycast الدولية وكما تم تثبيتها من قبل تفويضات DNSSEC التي تمت مع التفويضات الرئيسية لملف منطقة الجذر (ZSK) الخاص بـ IANA.

تتضمن الإنتقادات الموجهة لنظام خادم أسم الجذر الحالي والتأريخي نقص في مقاومة هجمة الحرمان الموزع للخدمة DDoS،مع الإشارة بإنه حتى مع شبكة anycast الحالية والواسعة النطاق من قبل كل مشغل لخادم أسم ملف الجذر فإنه لايزال ثمة بضع مئات فقط من خواد الأسم في العالم والتي تستطيع الرد بصورة رسمية لملف منطقة جذر DNS. نحن قلقون أيضاً بإن إمكانية الوصول الى نظام خادم أسم الجذر مطلوبة حتى في حالة الأتصال المحلي المحض، وإلا فإنه سوف لن يكون للعملاء المحليين خياراً لإكتشاف الخدمات المحلية. ففي عالم يسعى لنظام مصنّف مثل الإنترنت، لابد أن يتم توزيع الخدمات الهامة بصورة فائقة الجودة.

التفاصيل

هناك العديد من التغييرات المفيدة التي ينبغي بنائها. أولاً، شبكة anycast أولية ودولية ستسمح لأي مشغل لخادم أسم لإلتقاط حركة البيانات المتجهة نحو نظام خادم أسم الجذر وأن ترد عليه بشكل محلي. ستقوم IANA بإنشاء وبصورة رقمية وبمعية DNSSEC إصداراً إضافياً لملف منطقة الجذر التي تمتلك مجموعة مختلفة من سجلات NS في ذروتها. ستهب سجلات NS هذه بخوادم الأسم والتي لم يتم تفويض عناوينها لأي مشغل خادم جذر معين (RNSO) ولكن بدلاً من ذلك يتم تعليقها وفق الثقة الممنوحة لـ IANA لأجل الإستخدام من قبل أي أو كافة الأطراف المعنية. وستقوم IANA بتقديم طلب للمخصصات الصغيرة للبنية التحتية من قبل سجلات الإنترنت الأقليمية RIR(مثل ARIN و (APNIC، وعدة بادئات لـ IPv4 ذو 23 بايت وعدة بادئات لـ IPv6 ذو 48 بايت، للإستخدام في شبكة anycast الدولية لمنطقة الجذر.

وتغيير ثانٍ حول ملف منطقة الجذر الحالي الذي سيزود شبكة Anycast الدولية كما في اعلاه ولكن سيقوم بمنح خوادم الأسم التي تمتلك إتصال IPv6 فقط (المؤشرة بحضور سجلات AAAA) ولا إتصال IPv4 (المؤشرة بغياب سجلات A). سيسهّل التنوع البحث التشغيلي في تشبيك IPv6 فقط.

ومن شأن التغيّر الثالث الحاصل على ملف منطقة الجذر الحالية أن يوفر شبكة Anycast دولية ولكن سيتضمن تفويضات لكافة نطاقات new gTLDs المعروفة بما في ذلك غير المستعدة للتفويض (مثل CORP. و HOME.). سيتم تفويض هذه النطاقات gTLDs الى خادم إسم يتم تشغيله من قبل IANA نفسها لأغراض القياس. وسيتم تعيين كل gTLD بسجلات wildcard A وAAAA، والتي ستصل عناوينها الى خوادم الويب ويتم تشغيلها من قبل IANA لأغراض القياس.

التأثير

بالنظر للطبيعة الهرمية لموجه الإنترنت، يمكن أن يتم إعلان قوائم عناوين شبكة Anycast على عدة مستويات. قد يكون للجهاز الفعلي (VM, Virtual Machine) الذي يشتغل على حاسوب لابتوب عملية خادم الأسم الخاص به والذي يرصد العناوين المناسبة المعروفة بصورة جيدة، وفي هذه الحالة سوف لن تغادر إستعلامات خدمة أسم الجذر ذلك الجهاز الفعلي VM. قد يقوم جهاز الحاسوب المحمول (اللابتوب) أيضاً بإلتقاط حزم البيانات المتحركة نحو الخارج بإتجاه تلك العناوين المعروفة والتي تخدم أجهزة فعلية أخرى أو عمليات أخرى تشتغل على جهاز اللابتوب ذلك. قد يكون لجهاز التوجيه اللاسلكي النابع من جهاز الحاسوب المحمول هذا (اللابتوب) خوادم تنصت لتلك العناوين وفي هذه الحالة سوف لن تغادر أية إستفسارات خادم أسم التابع للشبكة الموقعية اللاسلكية (wirelss LAN). قد يقوم مزود خدمة الإنترنت ISP بتشغيل خوادم تنصت لتلك العناوين لخدمة أي أو كافة العملاء الذين لايقومون بتشغيل خوادمهم الخاصة بهم. وأخيراً، يتوقع من الإنترنت العالمية أن تمتلك عدة مشغلين الذي يعلنون عن موجهات لقوائم العناوين المعروفة تلك، وهي التي ستكون 12 مشغل موجود حالياً لخادم أسم الجذر.

وسيكون التأثير الإيجابي لهذا هو أن تكون هناك مرونة محتملة عالية وسيقل تأخير خدمة إسم الجذر. وسيكون التأثير السلبي لهذا هو أنه ستقل القدرة التشخيصية وزيادة التعرض الى ما يسمى "تسمم الطريق" أو " الإستيلاء أو سرقة" عبور خدمة إسم الجذر. ومن الأهمية بمكان إن يصبح التحقق من DNSSEC مألوفاً لأجل تقليل خسائر هذا النوع من الأستيلاء. نحن نسعى لأن نحمّل المهاجم عقوبةً بإن يكون " هو الضحية التي تخسر خدمة أسم الجذر" بدل من أن نرى " ضحية ترى فضاء أسم نظام DNS مختلف".

أمثلة

تظهر الأمثلة التالية سجل NS في ذروته وضع لكل ملف منطقة جذر مختلفة وتتضمن عنواناً. سوف يتم تضمين هذه البيانات في مختلف مناطق الجذر المختلف قبل توقيع DNSSEC وسيتم نشرها كملف "إشارات جذر". سيتم عرض البيانات المعروضة على موقع iana-servers.net في صفحة أخرى ملف المنطقة الحية على iana-servers.net. ستتطلب هذه الأمثلة أربعة تخصيصات صغير لبروتوكول IPv4 وست تخصيصات صغيرة لبروتوكول IPv6.

متغير 1: anycast الدولية

```
.IN NS anycast-1.iana-servers.net .
.IN NS anycast-1.iana-servers.net .
.ORIGIN iana-servers.net$
anycast-1 IN AAAA 2001:?:1::1
anycast-1 IN A ?.?.1.1
```

anycast-1 IN AAAA 2001:?:2::2
anycast-1 IN A ?.?.2.2

متغير 2: anycast الدولية لبروتوكل IPv6 فقط

.IN NS anycast-1.iana-servers.net .
.IN NS anycast-1.iana-servers.net .
.ORIGIN iana-servers.net$
anycast-1 IN AAAA 2001:?:3::1
anycast-1 IN AAAA 2001:?:4::2

متغير 3: anycast دراسة تضارب gTLD

.IN NS anycast-1.iana-servers.net .
.IN NS anycast-1.iana-servers.net .
.ORIGIN iana-servers.net$
anycast-1 IN AAAA 2001:?:5::1
anycast-1 IN A ?.?.5.1