خطة تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر

تقرير مسودة فريق التصميم - محدث في 4 أغسطس 2015

1 نظرة عامة

تحضر ICANN خطة لتنفيذ تغيير مفتاح الدخول الرئيسي (KSK) للتوقيع على إمتدادات أمان اسم النطاق DNSSEC لمنطقة الجذر. وتعمل ICANN بدورها وبصفتها مشغل وظائف IANA على التخطيط لتشغيل التغيير، وذلك بالتعاون مع شركاء إدارة ملفات منطقة الجذر (RZM). أما الشركاء فهم Verisign بصفتها مشرف منطقة الجذر، و الوكالة الوطنية الأمريكية للإتصالات والمعلومات (NTIA) التابعة لوزارة التجارة الأمريكية بصفتها مدير منطقة الجذر.[1]

كما ويشير تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر إلى تغيير المفتاح الذي جرى استخدامه منذ عام 2010 وذلك عندما تم التوقيع على منطقة الجذر بداية بموجب تعريف الامتدادات الأمنية لنظام اسم النطاق (DNSSEC)[2]. ويعني تغيير المفتاح إنشاء عنصر تشفير سري جديد وتوزيع عنصر عام جديد. حيث يعد توزيع العنصر العام الجديد بشكل مناسب الجانب الأكثر أهمية في عملية تغيير المفتاح.

تتوفر هذه الوثيقة للتعليق العام وتعتبر مشروع التقرير لمداولات فريق التصميم والذي يتألف من هيئة من الخبراء المتطوعين في نظام اسم النطاق DNS والامتدادات الأمنية لنظام اسم النطاق DNSSEC إلى جانب شركاء إدارة ملفات منطقة الجذر. وتكون حالة هذه الوثيقة مسودة ولك ليتم تعديلها عبر مساهمات من مجتمع الإنترنت خلال التعليقات العامة المفتوحة في ICANN ومداولات أخرى. وسيتم إصدار التقرير النهائي بعد إجراء المحادثات المترتبة.

2 قائمة المحتويات

[1] ويتم وضع مسودة الخطة بموجب و/أو اعترافاً بهيكل إدارة ملفات منطقة الجذر الحالية كما يمليها عقد وظائف IANA والاتفاقية التعاونية ما بين NTIA وVerisign في الوقت الراهن. ويعترف فريق التصميم وشركاء إدارة ملفات منطقة الجذر بأنه قد يترتب على جهود انتقال دور الإشراف على IANA الجارية تداعيات حول خطة تغيير متفاح التسجيل الرئيسي KSK ومشاركة NTIA في أية عملية في المستقبل. ومع ذلك، تستقل التفاصيل التقنية والاعتبارات إلى حد كبير عن جهود الانتقال المبذولة ونتائجها النهائية.

[2] راجع RFC 4033 وRFC 4034 وRFC 4035

3 الخلاصة التنفيذية

سعت ICANN بصفتها مشغل وظائف IANA وبالتعاون مع Verisign بصفتها مشرف منطقة الجذر والوكالة الوطنية الأمريكية للإتصالات والمعلومات (NTIA) التابعة لوزارة التجارة الأمريكية بصفتها مدير منطقة الجذر، والتي تعرف معاً باسم شركاء إدارة ملفات منطقة الجذر(RZM)، لوضع خطة لتشغير مفتاح الدخول الرئيسي (KSK) لمنطقة الجذر.

وبموجب الامتدادات الأمنية لنظام اسم النطاق DNSSEC، يستخدم مفتاح الدخول الرئيسي KSK لمنطقة الجذر لتسجيل مجموعة سجل مورد مفتاح نظام اسم النطاق DNSKEY. وتتضمن هذه المجموعة مفتاح تسجيل المنطقة (ZSK) والذي يستخدم لتسجيل كافة مجموعات سجل الموارد الأخرى (RRsets) في منطقة الجذر. كما ويشير تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر إلى تغيير المفتاح الذي جرى استخدامه منذ عام 2010 (وذلك عندما تم التوقيع على منطقة الجذر بداية بموجب الامتدادات الأمنية لنظام اسم النطاق DNSSEC). ويعني تغيير المفتاح إنشاء عنصر تشفير سري جديد وتوزيع عنصر عام جديد. حيث يعد توزيع العنصر العام الجديد بشكل مناسب الجانب الأكثر أهمية في تغيير المفتاح.

وطلبت ICANN في شهر ديسمبر 2014 متطوعين من المجتمع للمشاركة مع شركاء إدارة ملفات منطقة الجذر في فريق التصميم لوضع خطة تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر على النحو الوارد في هذه الوثيقة. وكانت الإنجازات المستهدفة لهذا العمل عبارة عن مجموعة شاملة من التوصيات التقنية والتشغيلية التي تهدف إلى توجيه شركاء إدارة ملفات منطقة الجذر في إنشاء خطة تنفيذ مفصلة لتنفيذ أول تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر. كما وينبغي مراجعة هذه الوثيقة باعتبارها خطة مشروع تهدف إلى تقديم هذه الإنجازات المستهدفة.

3.1 مصطلح نظام اسم النطاق DNS

تتعلق هذه الوثيقة بالتفاصيل التقنية لنظام اسم النطاق DNS والامتدادات الأمنية لنظام اسم النطاق DNSSEC. وبالتالي تتوفر تعريفات الامتدادات الأمنية لنظام اسم النطاق DNSSEC ذات الصلة (المصطلحات الدارجة) بسهولة، وتم إدراج التعريفات لبعض البنود ذات الصلة فيالجدول 1 أدناه.

المصطلح	المختصر	التوضيح
مجموعة سجل المورد	RRSet	مجموعة من البيانات المخزنة في نظام اسم النطاق DNS، وهي أصغر وحدة مسجلة حسب مفاتح الامتدادات الأمنية لنظام اسم النطاق DNSSEC
مفتاح الدخول الرئيسي	KSK	وهو زوج من المفاتيح العامة والخاصة[3] والتي يتمثل دورها في إنشاء توقيع قابل للتحقق بمجموعة من المفاتيح قيد الاستخدام في منطقة نظام اسم النطاق DNS. ويعتبر هذا الدور خاص وذلك لأن الامتدادات الأمنية لنظام اسم النطاق DNSSEC تتطلب هذا النوع من المفاتيح العامة ليتم توزيعها خارجياً إلى بروتوكول نظام اسم النطاق DNS
مفتاح تسجيل المنطقة	ZSK	وهو زوج من المفاتيح العامة والخاصة والتي يتمثل دورها في إنشاء توقيع لكافة مجموعات البيانات الأخرى في منطقة نظام اسم النطاق DNS. ولا يتم توزيع هذا المفتاح خارج بروتوكول نظام اسم النطاق DNS

[3] نيلز فريغسون، بروس شنير (2003). التشفير العملي. وايلي. ISBN 0-471-22357-3.

المصطلح	المختصر	التوضيح
DNSKEY RRset		وهي عبارة عن مجموعة من المفاتيح المستخدمة في منطقة ما، بما فيها أدوار مفتاح الدخول الرئيسي KSK ومفتاح تسجيل المنطقة ZSK، وهي مجموعة من سجلات مورد مفتاح نظام اسم النطاق DNSKEY
تغيير المفتاح		وهو إجراء التغيير من مفتاح تشفير إلى آخر على نحو منظم
مدقق (DNSSEC)		وهي برمجية تجري عمليات تدقيق أمنية على ردود الامتدادات الأمنية لنظام اسم النطاق DNSSEC، بما فيها التأكد من التوقيعات على البيانات كخطوة واحدة
مرتكز الثقة		وهو مفتاح تسجيل رئيسي عام مخزن موثوق تماماً من المدقق
تحديثات آلية لمرتكز الثقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC	RFC 5011	إحدى الطرق لتحديث مرتكزات الثقة تلقائياً في المدقق
التوقيع المزدوج		وهو إدراج توقيعين لمجموعة سجل المورد RRset، ويدرج المفتاح القديم والجديد عادة في التغيير. ويكون توقيع واحد في العادة كافي لمجموعة سجل المورد RRset
اللجنة الاستشارية لنظام خادم الجذر	RSSAC	وهي لجنة معتمدة في لوائح ICANN الداخلية وتقدم المشورة فيما يتعلق بنظام خادم ملف الجذر لمجتمع ICANN
آليات التمديد لنظام اسم النطاق DNS	EDNS or EDNS(0)	وهي محددة حالياً في RFC 6891، وتقدم وسائل لتمديد أو توسيع نموذج بروتوكول نظام اسم النطاق DNS. وتشير EDNS(0) إلى المجموعة الأولى من الامتدادات
سجل مورد موقّع التفويض	DS	وهو سجل الامتدادات الأمنية لنظام اسم النطاق DNSSEC يشير إلى مفتاح الدخول الرئيسي KSK المستخدم من خلال تفويض فرعي (أو لمنطقة الجذر، مفتاح الدخول الرئيسي KSK لنطاق المستوى الأعلى)
الرد بالنفي	NSEC أو NSEC3	تستخدم سجلات مورد الامتدادات الأمنية لنظام اسم النطاق DNSSEC المحدد للإشارة إلى عدم توفر البيانات على الأسئلة المطروحة
بيان ممارسات الامتدادات الأمنية لنظام اسم النطاق DNSSEC	DPS	وهي وثيقة تصف تفاصيل معالجة الامتدادات الأمنية لنظام اسم النطاق DNSSEC لمنطقة ما.

المصطلح	المختصر	التوضيح
مراسم المفتاح		وهي فعاليات يستخدم بها المفتاح الخاص داخل وحدة أمن الأجهزة HSM لإنشاء التوقيعات. وتستخدم عملية رسمية عندما يرغب المراقبون بمراقبة الممارسات.

الجدول 1. مصطلح نظام اسم النطاق DNS والامتدادات الأمنية لنظام اسم النطاق DNSSEC

3.2 مصطلحات أمنية أخرى

المصطلح	المختصر	التوضيح
OpenPGP	OpenPGP	وهي وسائل لإدارة المفاتيح العامة والخاصة. RFC 4880: صيغة رسالة OpenPGP
معيار صياغة رسالة التشفير	PKCS#7	RFC 2315 :PKCS #7: صياغة رسالة التشفير – النسخة 1.5
الدليل - المفتاح العام وأطر عمل شهادة الخصائص	X.509	معيار قطاع معايير الاتصالات في الاتحاد الدولي للاتصالات ITU-T لإدارة المفاتيح العامة والخاصة. توصية قطاع معايير الاتصالات في الاتحاد الدولي للاتصالات | ITU-T X.509 ISO/IEC 9594-8
طلب تسجيل المفتاح	KSR	وهو هيكل البيانات ويتكون من طلبات الحصول على توقيعات على المفاتيح، وبالأخص مجموعات مفتاح نظام اسم النطاق DNSKEY ليوقع عليها مفتاح تسجيل الدخول
رد المفتاح الموقع	SKR	وهو هيكل البيانات ويتكون من توقيعات مفتاح خاص مستحدث، وبالأخص توقيعات مفتاح تسجيل الدخول KSK على مجموعات مفتاح نظام اسم النطاق DNSKEY

الجدول 2. مصطلحات أمنية أخرى

3.3 مصطلحات شبكية أخرى

تستخدم بعض المصطلحات الأخرى أكثر مما يحتاجه التعريف للجمهور العام

المصطلح	المختصر	التوضيح
بروتوكول مخطط المستخدم	UDP	وهو بروتوكول نقل مستقل عن السياق بأفضل جهد لإرسال البيانات عبر الإنترنت
بروتوكول التحكم بالإرسال	TCP	وهو بروتوكول نقل ذو نظام ثماني مضمون موجه بالاتصل لإرسال البيانات عبر الإنترنت

المصطلح	المختصر	التوضيح
وحدة النقل القصوى	MTU	وهي أقصى عدد من المجموعات الثمانية والذي قد يكون في بيانات مرسلة عبر جزء من الإنترنت، ويشير مسار وحدة النقل القصوى MTU إلى أدنى وحدة نقل قصوى لكافة الأجزاء المستخدمة في طرف كامل عبر الإنترنت

الجدول 3. مصطلحات شبكية أخرى

3.4 ملخص التوصيات

التوصية 1: ينبغي أن يتبع تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر الإجراءات الواردة في RFC 5011 لتحديث مرتكزات الثقة خلال تغيير مفتاح الدخول الرئيسي.

التوصية 2: ينبغي على ICANN تحديد موردين برمجيات مفتاح نظام اسم النطاق DNS والعمل عن كثب معهم لإعطاء العمليات شكل محدد لضمان قوة وأمان توزيع مرتكز الثقة باستخدام قنوات مورد معين.

التوصية 3: ينبغي على ICANN تحديد مكاملي نظم مفتاح نظام اسم النطاق DNS والعمل معهم عن كثب لإعطاء العمليات شكل محدد لضمان قوة وأمان توزيع مرتكز الثقة باستخدام قنوات مكامل محددة.

التوصية 4: ينبغي على ICANN إتخاذ دور فعّال في تعزيز مصادقة مرتكز الثقة في منطقة الجذر، بما فيها تسليط الضوء على المعلومات المنشورة في موقع IANA الخاص بـ ICANN.

التوصية 5: ينبغي ألا يتطلب تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر تغييرات جوهرية على إدارة مفتاح الدخول الرئيسي KSK الحالي واستخدام العمليات من أجل إبقاء مستويات عالية من الشفافية المرتبطة بهم.

التوصية 6: ينبغي أن تتماشى كافة تغييرات مجموعات سجل المورد لمفتاح نظام اسم النطاق DNSKEY في منطقة الجذر مع فترات زمنية لمدة 10 أيام واردة في بيان ممارس DNSSEC لمشغلات مفتاح الدخول الرئيسي KSK.

التوصية 7: ينبغي المحافظة على الخوارزمية الحالية وحجم المفتاح لمفتاح الدخول الرئيسي KSK المقبل بالنسبة لتغيير أول مفتاح الدخول الرئيسي KSK لمنطقة الجذر.

التوصية 8: ينبغي مراجعة خيار الخوارزمية وحجم المفتاح في المستقبل بالنسبة لتغييرات مفتاح الدخول الرئيسي KSK لمنطقة الجذر التالية.

التوصية 9: ينبغي على ICANN وبالتعاون مع شركاء إدارة ملفات منطقة الجذر تصميم وتنفيذ خطة الاتصالات لزيادة الوعي بتغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر، بما فيها التواصل مع المجتمع التقني العالمي من خلال اجتماعات تقنية مناسبة ومع "شركاء القناة" كما أولئك الواردين في هذه الوثيقة.

التوصية 10: ينبغي على ICANN أن تطلب من اللجنة الاستشارية لنظام خادم الجذر RSSAC تنسيق مراجعة بالجدول الزمني المفصل بالنسبة لمدة تغيير مفتاح تسجيل الدخول KSK قبل أن يتم نشرها، وينبغي احتواء الطلبات المعقولة لتعديل ذلك الجدول الزمني في الحدث بحيث يحدد أي مشغل خادم جذر أسباب تشغيلية للقيام بذلك.

التوصية 11: ينبغي على ICANN التعاون مع اللجنة الاستشارية لنظام خادم الجذر RSSAC وشركاء إدارة ملفات منطقة الجذر RZM لضمان استخدام قنوات الاتصالات في الوقت الحقيقي وذلك للتأكد من الوعي التشغيلي المناسب بنظام خادم ملف الجذر لكل تغيير حاصل في منطقة الجذر والذي يتضمن إضافة أو إزالة مفتاح الدخول الرئيسي.

التوصية 12: ينبغي على ICANN التعاون مع اللجنة الاستشارية لنظام خادم الجذر RSSAC لطلب تنفيذ مشغلات خادم الجذر مجموعة البيانات حيث ستبلغ عن التحليل التالي وتساعد في وصف التأثير التشغيلي المترتب على تغيير مفتاح الدخول الرئيسي، وبأنه يجب توفير الخطط والمنتجات لمجموعة البيانات تلك وذلك للحصول على تحليل الطرف الثالث.

التوصية 13: ينبغي على شركاء إدارة ملفات منطقة الجذر RZM ضمان تنسيق أية زيادة مستقبلية في حجم مفتاح تسجيل الجذر ZSK بدقة مع مغيري مفتاح الدخول الرئيسي، كأن لا يتم تنفيذ العملتين بشكل متزامن.

التوصية 14: وللحد من وقت التعافي نظراً لصعوبة إشراك مفتاح الدخول الرئيسي KSK المقبل، ينبغي إنشاء رد المفتاح الموقّع SKR المنشى فقط عبر مفتاح الدخول الرئيسي KSK الحالي بالتوازي مع رد المفتاح الموقّع SKR المنشئ عبر مفتاح الدخول الرئيسي KSK الحالي.

التوصية 15: ينبغي على شركاء إدارة ملفات منطقة الجذر RZM وضع وتوثيق عملية استخدام رد المفتاح الموقّع SKR المنشى لمفتاح الدخول الرئيسي KSK الحالي.

3.5 الجمهور

تستهدف هذه الوثيقة الجمهور التقني، وبالأخص الجمهور المعتاد على نظام اسم النطاق DNS وبروتوكولات الامتدادات الأمنية لنظام اسم النطاق DNSSEC، والجوانب التشغيلية لنظام اسم النطاق DNS، والعمليات المرتبطة باستخدام الامتدادات الأمنية لنظام اسم النطاق DNSSEC في منطقة الجذر.

3.6 نطاق الوثيقة

تهدف هذه الوثيقة لصياغة وتقديم مجموعة من التوصيات التي توجه شركاء إدارة ملفات منطقة الجذر في وضعهم خطة تنفيذ مفصلة لتغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر.

4 تاريخ مختصر

4.1 نشر الامتدادات الأمنية لنظام اسم النطاق DNSSEC في منطقة الجذر

تعاون شركاء إدارة ملفات منطقة الجذر RZM عام 2009[4] لنشر الامتدادات الأمنية لنظام اسم النطاق DNSSEC في منطقة الجذر، والتي بلغت ذروتها في أول نشر لمنطقة الجذر الموقعة والقابلة للمصادقة في يوليو 2010. وتم إنشاء مفتاح الدخول الرئيسي KSK لمنطقة الجذر المستخدم حالياً في أول مراسيم مفتاح الدخول الرئيسي KSK المنعقد في مرفق الإدارة الرئيسي (KMF) والذي تديره ICANN في مدينة كولبيبر في ولاية فيرجينيا الأمريكية. تم نقل المواد الرئيسية فيما بعد إلا مرفق الإدارة الرئيسي KMF الثاني لـ ICANN في إلسيجوندو في ولاية كاليفورنيا الأمريكية وبمجرد ما تم التحقق من انتقالها بشكل آمن، تم نشر الجزء العام من مفتاح الدخول الرئيسي KSK في منطقة الجذر وبصفتها مرتكزات الثقة.

[4] تم نشر توزيع تفاصيل الامتدادات الأمنية لنظام اسم النطاق DNSSEC المفصلة في منطقة الجذر على الموقع http://www.root-dnssec.org/

وتم تحديد المتطلبات لإنشاء مفتاح تسجيل الدخول KSK في منطقة الجذر بالإضافة إلى المسؤوليات المنوطة بكل من شركاء إدارة ملفات منطقة الجذر RZM من خلال NTIA[5]. وتم نشر الإجراءات حيث استوفى مشرف منطقة الجذر ومشغل وظائف IANA هذه المتطلبات في بيان ممارسة وسياسة الامتدادات الأمنية لنظام اسم النطاق DNSSEC (DPS) المنفصلة[6].

تم تعديل عقد وظائف IANA ما بين NTIA وICANN في يوليو 2010 لإدراج المسؤوليات المرتبطة بإدارة مفتاح الدخول الرئيسي KSK في منطقة الجذر، وتم تنفيذ تلك المتطلبات المرحلة في المراجعات اللاحقة من ذلك العقد[7]. وتم تعديل الإتفاقية التعاونية ما بين NTIA وVerisign كذلك في يوليو 2010 لعكس مسؤوليات مشغل مفتاح تسجيل منطقة الجذر ZSK لـ Verisign.[8]

يتطلب عقد وظائف IANA من ICANN إجراء تغيير مفتاح الدخول الرئيسي لمنطقة الجذر، إلا أنه لا يحدد الجدول الزمني المفصل أو الخطة التنفيذية. يتكون بيان ممارسات الامتدادات الأمنية لنظام اسم النطاق DNSSEC لمشغل مفتاح الدخول الرئيسي KSK لمنطقة الجذر على هذا البيان، بوضع متطلب للتغيير في قسم 6.5:

"سيتم تحديد كل مفتاح تسجيل رئيسي KSK لمنطقة الجذر لتغييره عبر مراسم المفتاح كما هو مطلوب، أو بعد خمس سنوات من التشغيل."

4.2 التعليق العام لتغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر

قامت ICANN في 8 مارس 2013 بفتح فترة التعليق العام لطلب الملاحظات المتعلقة بتنفيذ مفتاح الدخول الرئيسي KSK لمنطقة الجذر[9]. وأجابت ست منظمات و15 فرد. وقد حددت ICANN في ملخصها على الردود[10] سبع توصيات لشركاء إدارة ملفات منطقة الجذر RZM وذلك للنظر فيها:

1. ينبغي إنشاء مجموعة من الاختبارات والتدابير مع قاعدة اختبار قبل الشروع في تغيير مفتاح الدخول الرئيسي KSK RFC 5011. يستلزم إنشاء خطوط الاتصال أثناء طرق ومراحل الاختبار للحصول على تقييم مبني ناجح.
2. وينبغي إجراء تغيير مفتاح الدخول الرئيسي KSK عملياً في أقرب وقت ممكن مع التشديد على الاستعداد|.
3. وينبغي تنفيذ التدابير والمراقبة التي تتكون من نموذجين رئيسين بارزتين لقياس التأثير [التقني والمستخدم النهائي] لتغيير مفتاح الدخول الرئيسي KSK.
4. ويجب إجراء تغيير مفتاح الدخول الرئيسي KSK بشكل منتظم.
5. ويجب تقديم الإشعارات العامة لمجموعات أصحاب مصلحة متنوعة ومتعددة قبل حدث تغيير مفتاح الدخول الرئيسي KSK، وذلك لتقديم إشعار هام مقدماً.
6. ويستلزم إجراء المزيد من التحقيات حول الاستقرار التشغيلي وتغييرات مفتاح الدخول الرئيسي KSK المتكررة و[الاحتمالية وتأثير] عدم الامتثال بـ RFC 5011.

---

[5] "متطلبات الاختبار والتنفيذ لنشر الامتدادات الأمنية لنظام اسم النطاق DNSSEC الأولي في منطقة الجذر الرسمية"، 29 أكتوبر 2009
http://www.ntia.doc.gov/files/ntia/publications/dnssec_requirements_102909.pdf

[6] https://www.verisigninc.com/en_US/repository/index.xhtml،https://www.iana.org/dnssec

[7] http://www.ntia.doc.gov/page/iana-functions-purchase-order

[8] http://www.ntia.doc.gov/files/ntia/publications/amendment31_07062010.pdf

[9] https://www.icann.org/public-comments/root-zone-consultation-2013-03-08-en

[10] https://www.icann.org/en/system/files/files/report-comments-root-zone-consultation-08apr14-en.pdf

4.3 المناقشة الأولية لتغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر في 2013

عقد شركاء إدارة ملفات منطقة الجذر RZM اجتماعاً في أواخر شهر يوليو 2013 لمناقشة خيارات لتغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر. وحدد الفريق الحاجة لإجراء تغيير المفتاح وذلك لتنفيذه في خطوات متميزة من خلال فترة زمنية متحفظة ومزايا توعية المجتمع على نطاق واسع وفكرة جدول تغيير RFC 5011 المعدل مع إلغاء التأجيل. وتم تقديم هذه المبادئ على مستوى عالي في اجتماع فريق عمل عمليات نظام أسم النطاق (DNSOP) لفريق عمل هندسة الإنترنت لدى فريق عمل هندسة الإنترنت IETF 87[11].

4.4 مشورة اللجنة الاستشارية للأمان والاستقرار المتعلقة بتغيير مفتاح DNSSEC في منطقة الجذر

نشرت اللجنة الاستشارية للأمن والاستقرار (SSAC) في ICANN في شهر نوفمبر 2013 SAC063[12] بشأن تغيير مفتاح الدخول الرئيسي KSK. وشمل التقرير المخاطر التي تنطوي عليها فضلاً عن قاعدة الرمز في ذلك الحين (وبالأخص عمليات تنفيذ نظام اسم النطاق DNS مفتوحة المصدر). وأوصى التقرير بإجراء اتصال لنشر تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر، حيث شجعت على إجراء اختبار لتجميع وتحليل سلوكيات المحلل، وإنشاء مقاييس لما من شأنها أن تكون مستويات مقبولة من "الانقطاع" في تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر، وتعريف تدابير الاسترجاع في حالة "الانقطاع" المفرط"، ومجموعة من المعلومات للإبلاغ عن عمليات تغيير مفتاح من هذا النوع مستقبلاً.

سلط تقرير اللجنة الاستشارية للأمن والاستقرار SSAC الضوء على ثلاثة مواضيع والتي ستتم تغطيتها في هذه الوثيقة لاحقاً. أولاً، قد يؤثر التقدير التقريبي بنسبة 1.1% لأولئك الذين يعتمدون على تمكين الامتدادات الأمنية لنظام اسم النطاق DNSSEC لنظام اسم النطاق DNS بشكل سلبي عبر تغيير مفتاح الدخول الرئيسي لمنطقة الجذر بتوجيه جيد. ثانياً، تعتبر حالة الدعم لتحديثات مرتكز ثقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC التلقائي، والمعروف باسم RFC 5011، موجودة إلا أنه لا يمكن التنبؤ بها. وثالثاً، أُعتقد بأن حجم ردود نظام اسم النطاق DNS يشكل قلقاً عندما يتعلق الأمر بحدوث تجزئة حزمة بروتوكول مخطط المستخدم UDP الأساسية وإرجاعها إلى استفسارات بروتوكول التحكم بالإرسال TCP.

4.5 جمع ICANN فريق تصميم تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر

وطلبت ICANN في شهر ديسمبر 2014 متطوعين من المجتمع للمشاركة مع شركاء إدارة ملفات منطقة الجذر في فريق التصميم لوضع خطة تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر على النحو الوارد في هذه الوثيقة.

5 وصف تغيير مفتاح الدخول الرئيسي KSK على مستوى عالي

تتبع الخطة المنبثقة في شهر يوليو 2013، وهو أمر غير بعيد عن إزالته من الخطط لتغيير أي مفتاح تسجيل رئيسي آخر هذه الخطوات:

1) إنشاء زوج مفاتيح مفتاح الدخول الرئيسي KSK المقبل (العام والخاص).

2) استبدال المفتاح العام لمفتاح الدخول الرئيسي KSK المقبل في منطقة الجذر و/أو متوفر للأطراف المعوّل عليها.

[11] http://www.ietf.org/proceedings/87/slides/slides-87-dnsop-6.pdf
[12] https://www.icann.org/en/system/files/files/sac-063-en.pdf

3) ينفذ المفتاح العام لمفتاح الدخول الرئيسي KSK لمنطقة الجذر الجديد، وبالانحراف عن المناطق الأخرى، في حالة عندما تصبح مقبولة من كافة الأطراف المعنية والتي تعتبر مفتاح الدخول الرئيسي KSK التالي في الواقع.
وبالإضافة إلى قبولها بشكل سلبي، فإن المفتاح العام لمفتاح الدخول الرئيسي KSK لمنطقة الجذر الجديد متوفر على الوسائط الإلكترونية أو غير الإلكترونية وذلك لتسمح لمشغلي المحلل والمطورين ممن لديهم خوادم لا تدعم مدة RFC 5011 بإدراج مرتكز ثقة جديد في أنظمتهم ومنتجاتهم. (أما بالنسبة لـ "المناطق الأخرى"، فإنه يتم استبدال هذه الخطوة بإبلاغ حامل سجل التوقيع الرقمي بأنه يوجد مفتاح تسجيل رئيسي KSK مقبل.)

4) وتتبدل عملية التوقيع من استخدام المفتاح الخاص لمفتاح الدخول الرئيسي KSK الحالي إلى المفتاح الخاص لمفتاح الدخول الرئيسي KSK المقبل.

5) ويعتبر مفتاح الدخول الرئيسي KSK المقبل في حالة الانتقال حالياً حيث تنتهي مدة التوقيعات الناشئة من مفتاح الدخول الرئيسي KSK المقبل أو تختفي من وجهة نظر التشغيل.

6) وتتم إزالة المفتاح العام لمفتاح الدخول الرئيسي KSK الحالي من منطقة الجذر (دون إلغاءها).

7) وبالانحراف عن عمليات التشغيل الاعتيادية، فإنه يعاد تقديم مفتاح الدخول الرئيسي KSK لمنطقة الجذر الحالية بهدف وضع علامة إلغاء عليه حسب توجيهات RFC 5011. ويتم تصميم هذه الخطوة المنفصلة لاستيعاب عمليات تشغيل مفتاح تسجيل منطقة الجذر ZSK، والتي تتضمن تغيير ذلك المفتاح دون المبالغة في تحجيم ردود نظام اسم النطاق DNS بالنسبة لمجموعة مفتاح منطقة الجذر المكتمل.

6 نهج فريق التصميم

نظر فريق التصميم في جوانب عدة من تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر، والتوصيات الصادرة من كل جانب من الدراسة لتوجيه وضع خطة تنفيذ عبر شركاء منطقة الجذر.

- الاعتبارات التشغيلية: التأثير المترتب على مستخدمي الإنترنت النهائين ومشغلي أنظمة نظام اسم النطاق DNS والخدمات المستخدمة عبر أولئك المستخدمين النهائين
- اعتبارات البروتوكول: المدى الذي يكون فيه عناصر البروتوكول الموثق الحالي كافي لاستيعاب تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر
- التأثير على إدارة مفتاح الدخول الرئيسي KSK لمنطقة الجذر: التأثير على العمليات المشاركة في إدارة مفتاح الدخول الرئيسي KSK من خلال مشغل وظائف IANA
- اعتبارات التشفير: التأكد من احتواء النظام بأكمله قوة تشفير كافية
- التواصل والتنسيق مع كافة الأطراف المشاركة.

يتم اكتشاف كل من هذه الجوانب فردياً في الأقسام التالية. كما ويقدم حل تغيير تقني مفصل كتوضيح لطريقة اتباع التوصيات، ويقصد منه كنقطة بداية لشركاء إدارة ملفات منطقة الجذر RZM بينما يستكملون خطتهم التنفيذية.

6.1 الاعتبارات التشغيلية

من المتوقع حدوث التأثير على مستخدمي الإنترنت النهائين ومشغلي أنظمة نظام اسم النطاق DNS أثناء هاتين الخطوتين في الأعلى. وعندما تتم إضافة المفتاح العام لمفتاح التشغيل الرئيسي KSK المقبل إلى منطقة الجذر، فإن حجم الرد على جذر مفتاح نظام اسم النطاق DNSKEY سيتنامى. وعندما لا ينشئ المفتاح الخاص لمفتاح الدخول الرئيسي KSK الحالي أي توقيعات، فإن التحقق باستخدام ذلك المفتاح العام سيتوقف عن العمل كما هو متوقع.

ومن المحتمل مع الردود الموسعة على مفتاح نظام اسم النطاق DNSKEY بأن تحدث تجزئة حزم بروتوكول مخطط المستخدم UDP مع نتائج مختلفة قليلاً على الاصدار الرابع من بروتوكول الانترنت IPv4 والاصدار السادس من بروتوكول الانترنت IPv6. ويوجد بالفعل عناصر إنترنت تنظر إلى الأجزاء على أنها ذات طبيعة غريبة وتصفيها. أما بالنسبة لنظام اسم النطاق DNS والذي لا يحتفظ بحالة ما فيما يتعلق بالردود المرسلة، فهذا يعني بأنه ربما لم يحصل العميل على الرد المتوقع. وثمة احتمالية كذلك لتخطي رد بروتوكول مخطط المستخدم UDP الكبير الاستفسار عن حجم مخزن حمولة نظام اسم النطاق DNS المحددة، وبالتالي زيادة مستوى الردود المقتطعة وإعادة الاستفسار اللاحق باستخدام بروتوكول التحكم بالإرسال TCP.

وبمجرد لم يعد مفتاح الدخول الرئيسي KSK الحالي يوقع على مفتاح تسجيل المنطقة، ومع المغزى بأن مفتاح الدخول الرئيسي KSK المقبل ينشئ توقيعات، سيفشل محقق الامتدادات الأمنية لنظام اسم النطاق DNSSEC مع مفتاح الدخول الرئيسي KSK الحالي فقط المهيء على أنه مرتكز ثقة في مصادقة ردود الامتدادات الأمنية لنظام اسم النطاق DNSSEC الموقّع. وما تعنيه سوف "يفشل" المحقق بأنه سينظر في كافة ردود نظام اسم النطاق DNS الموقعة على أنها غير صحيحة.

ولن يتمكن العميل النهائي الذي يستخدم حلول التحقق على وجه الحصر حيث يفشل في اختيار مفتاح الدخول الرئيسي KSK المقبل، أو يفشل في تلقي ردوداً أكبر خلال عمليات تغيير المفتاح، من مصادقة أية ردود نظام اسم نطاق DNS موقّع. وسوف يبدو الأمر للعميل النهائي على شكل انقطاع الإنترنت حيث لا يتم حل أسماء النطاق. وعندما تحدث حالات مشابهة من قبل، تزداد مطالبات التأثير الجانبي على مراكز دعم العميل، والذي يفرض عبء إضافي على دعم عملاء مزودي خدمات الإنترنت وأدوار الإدارة التشغيلية.

ينبغي على ICANN تنسيق اتصالات الخطة مع تقديم مفتاح الدخول الرئيسي KSK المقبل، بالإضافة إلى التغيير من مفتاح الدخول الرئيسي KSK الحالي إلى المقبل لإنشاء التوقيع (راجع التوصية 8).

6.2 اعتبارات البروتوكول

6.2.1 تهيئة مرتكز ثقة منطقة الجذر

يوجد نوعين من تهيئة مرتكز الثقة لأخذها في الاعتبار:

- مرتكزات الثقة في حلول التصديق عبر الإنترنت
- مرتكزات الثقة في الأجهزة/الأنظمة التي غير متصلة بالإنترنت أثناء التغيير وإعادة إتصالها بالإنترنت لاحقاً

قد تستخدم حلول المصادقة عبر الإنترنت تحديثات تلقائية لمرتكزات ثقة الامتدادات الأمنية لنظام اسم النطاق (DNSSEC) كما هو موصوف في RFC 5011، في حال دعمت برمجيات نظام اسم النطاق DNS المستخدمة هذه الآلية وتم تهيئتها لاستخدام هذه الآلية لتحديث مفتاح الدخول الرئيسي لمنطقة الجذر.

وسوف تحتاج حلول المصادقة عبر الإنترنت الغير قادرة أو التي لا ترغب باستخدام التحديثات التلقائية لمرتكزات ثقة أمن نظام اسم النطاق DNS إلى تحديثها يدوياً أثناء تغيير مفتاح الدخول الرئيسي. وينبغي أن يتبع التحديث اليدوي توقيت آلية RFC 5011 - ويجب إضافة مرتكز الثقة الجديد إلى تهيئة محلل المصادقة هذا في فترة نشر التغيير (راجع القسم 11 للحصول على التفاصيل)، ولا يجب إزالة مرتكز الثقة الحالي قبل توقيع منطقة الجذر مع مفتاح الدخول الرئيسي KSK لمنطقة الجذر الحالي. وعلاوة على ذلك، ينبغي ألا تتم إزالة مرتكز الثقة الحالي قبل إلغاء مفتاح الدخول الرئيسي KSK لمنطقة الجذر الحالي، وذلك من حيث الممارسة التشغيلية الحكيمة التالية. وتعتبر آليات استرداد مرتكز الثقة الجديد مشابه للأجهزة غير المتصلة بالإنترنت والموصوفة أدناه.

التوصية 1: ينبغي أن يتبع تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر الإجراءات الواردة في RFC 5011 لتحديث مرتكزات الثقة خلال تغيير مفتاح الدخول الرئيسي.

يتعين تحديث الأجهزة الغير متصلة بالإنترنت أثناء تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر بشكل يدوي في حال إعادة اتصالها بالإنترنت بعد استكمال التغيير. ويجب تشغيل هذه الأجهزة بالأساس كما لو أنه تم تثبيتها حديثاً.

ينبغي أن تتبع العملية التي يستعد بها أي جهاز ليتمكن من إجراء مصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC بشكل أكثر عموماً نهج يخفف الفرصة لاستخدام مرتكز ثقة غير مناسب. ويجري تعميم المشورة العامة لهذا النوع من الأجهزة حالياً في مسودة إنترنت، تحت عنوان "نشر مرتكز ثقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC لمنطقة الجذر" ضمن فريق عمل هندسة الإنترنت IETF[13]، إلا أنه يتطلب مزيداً من المراجعة من أجل التوصل إلى وثيقة إجماع ثابتة تقدم المشورة للمنفذين.

يدعم فريق التصميم مناقشة المجتمع ومراجعته لمسودة الإنترنت ضمن فريق عمل هندسة الإنترنت IETF، مع هدف نشر مواصفة ثابتة قائمة على مراجعة الأقران في مجموعة طلب الحصول على التعليقات RFC.

ثمة حالات استخدام متعددة لاسترجاع مرتكزات ثقة حديثة، والتي تم كشفها بشكل مختصر أدناه.

6.2.1.1 مزيد من المناقشة في RFC 5011

ذكر في النص السابق محللات "غير قادر أو غير راغب" للاعتماد على نهج RFC 5011. وما يقصد بهذا القسم تقديم معلومات أساسية حول تلك المرحلة.

حيث يعتبر روح مؤقت ركيزة RFC 5011 إضافية أمر مهم. ويتم إدراج المؤقت لمنع قبول المفتاح المقدم بشكل خاطئ. وبعبارة أخرى، إذا أرادت جهة ما تقديم مفتاح تسجيل رئيسي KSK خاطئ، فربما تنجح في نشر المفتاح. وفي تلك الحالة، ستتمكن السلطة الحقيقية من التنازل عن المفتاح الخاطئ قبل أن يتم دمج الاعتماد فيها.

ولا تعتمد مقاومة RFC 5011 في المحللات على أسئلة مرتبطة بتصميم الآلية المستحدثة. بل تتجذر المقاومة بالأحرى في بضعة حقائق تشغيلية. تشكل إدارة التهيئة قلق كبير عند تشغيل مجموعة من الخوادم والاعتماد على "الدفع نحو خارج" ملفات التهيئة المدارة. وتتعارض آلية تحديث RFC 5011 مع ذلك، مع اكتساب مجموعة الآليات المهيئة معلومات جديدة، والتي تختلف عن التهيئة المدارة مركزياً.

وبمراعاة ذلك، ستجري المشغلات الكبيرة عملية يدوية، وهي عملية من شأنها الاستفادة من آليات تلقائية عدة. وقد يكون نظام تلقائي واحد بمثابة وسيلة تتبع آلية تحديث RFC 5011. وفي استطلاع غير رسمي موجز، ستعتمد المشغلات الكبيرة على تحري مفتاح الدخول الرئيسي لمنطقة الجذر الجديد بضعة طرق مختلفة بما فيها الاتصال البشري لإنشاء الثقة. وهذا هو السبب لاقتراح بدائل لـ RFC 5011.

[13] http://tools.ietf.org/html/draft-jabley-dnsop-validator-bootstrap-00

وللغوص أعمق في تشغيل RFC 5011، فقد تم تحديد بضعة فجوات. وتتضمن الفجوة الأولى تحقق عملية RFC 5011 الناجحة عن بعد. أما الفجوة الثانية تتضمن القدرة على نشر الاختبار في خضم مؤقت الركيزة الإضافية.

أما المطلوب فهو تعريف وسائل استخدام مرتكزات الثقة لدى المحلل بمصدر الثقة. وبالنظر إلى خلفية المراقبة المتفشية، لا يكمن المغزى بمعرفة تهيئة وإمكانيات محلل معين، بل للتأكيد أولاً على أنه تم اتباع عملية RFC 5011 بشكل كافي والحصول على فكرة عن موعد قبولها للالتزام بمفتاح الدخول الرئيسي KSK لمنطقة الجذر المقبلة.

وتحديد الحاجة كذلك لتسريع القدرة على إجراء فحص وظيفي، فحص يظهر حدوث خطوات RFC 5011 على الرغم من الالتزام بنموذج الأمن المطلوب. وتحتاج الوسائل على وجه التحديد التمكن من تجاوز مؤقت المرتكز الإضافي المحدد للسماح بإجراء ضبط أقصر أثناء الاختبار. يعد تقديم آلية "الاختبار الآمن" لضمان أنه لن يتم استخدام اختبار مؤقت التركيز الإضافي في الإنتاج أمر مرغوب. وهو بمثابة اقتراح يستهدف مطوري الأداة وموردي برمجيات نظام اسم النطاق DNS.

6.2.1.2 تنسيقات مرتكز الثقة الأخرى

منذ التوقيع الأولى على منطقة الجذر، وفرت ICANN مرتكز الثقة في تنسيقات دون نظام اسم النطاق DNS عبر شبكة الإنترنت[14]. وتقدم مرتكزات الثقة هذه وسائل بمسار غير حرج لتوزيع وتقديم مرتكز ثقة منطقة الجذر، أي، وسائل خارج عمليات نظام اسم النطاق DNS. (يتطلب الموقع الإلكتروني الدخول إلى نظام اسم النطاق DNS للوصول إلى الملفات.) وبالنظر إلى اعتبار المسار غير الحرج، فمن الممكن توزيع مرتكزات ثقة جديدة. ومن الممكن إضافة مرتكزات ثقة في مرحلة ما مستقبلاً على خوارزميات تشفير امتدادات أمنية لنظام اسم النطاق DNSSEC مختلفة[15] وذلك للتأكيد على الإمكانيات الجديدة المطلوبة. وقد تكون هذه أيضاً وسائل لما قبل توسيع المحللات قبل تغيير ناجم عن حالة طارئة.

6.2.1.3 موردي برمجيات نظام اسم النطاق DNS

قد يتم تجميع مرتكزات الثقة مع برمجيات نظام اسم النطاق DNS عن طريق موردها (إما عبر مصدر مفتوح أو شخصي/تجاري). ويتعين على مورد البرمجيات إصدار نسخة جديدة من مجموعة مرتكز الثقة لإبقاء البرمجيات الحالية.

ومن المهم أن توزيع مرتكزات الثقة بهذا الأسلوب موثوق به، والاستفادة من أياً كانت آليات المصادقة المتوفرة بالفعل لضمان نزاهة البرمجية على النظام النهائي. ويتطلب موردي البرمجيات وسيلة قوية وفعالة لضمان الوثوق بمرتكزات الثقة التي يوزعونها مع برمجياتهم، بما أنه من المحتمل أن يكون تأثير توزيع مفاتيح غير موثوقة أمر هام، وبالأخص إذا تم توقيعها بمفاتيح تسجيل الرمز باعتبارها جزء من استراتيجية تحديث برمجيات المورد.

التوصية 2: ينبغي على ICANN تحديد موردين برمجيات مفتاح نظام اسم النطاق DNS والعمل عن كثب معهم لإعطاء العمليات شكل محدد لضمان قوة وأمان توزيع مرتكز الثقة باستخدام قنوات مورد معين.

6.2.1.4 خبراء تكامل الأنظمة

تعتبر من إحدى وسائل توزيع مرتكزات ثقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC عبر مكامل الأنظمة، على سبيل المثال، مشرف الحزمة أو مورد نظام التشغيل. وفي هذه الحالة، سيقدم مكامل الأنظمة حزم مستحدثة لكافة نسخ مرتكزات الثقة في النظام. فثمة جهود مبذولة في توزيعات لينكس المتعددة لتقديم حزمة بإحدى نسخ مرتكز الثقة الموثوق.

[14] https://www.iana.org/dnssec/files

[15] https://www.iana.org/assignments/dns-sec-alg-numbers/dns-sec-alg-numbers.xhtml#dns-sec-alg-numbers-1

التوصية 3: ينبغي على ICANN تحديد مكاملي نظم مفتاح نظام اسم النطاق DNS والعمل معهم عن كثب لإعطاء العمليات شكل محدد لضمان قوة وأمان توزيع مرتكز الثقة باستخدام قنوات مكامل محددة.

6.2.1.5 مدراء النظام

بإمكان مدراء الأنظمة تحميل مرتكزات ثقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC يدوياً من موقع IANA التابع لـ ICANN أثناء تثبيت أو تحديث البرمجية. ويتم تقديم مرتكزات ثقة منطقة الجذر الحالية من خلال مشغل وظائف IANA على الموقع المخصص[16] للحصول على معلومات تتعلق بالامتدادات الأمنية لنظام اسم النطاق DNSSEC في منطقة الجذر. ويعد تحديد موثوقية تحميل مرتكز الثقة أمر هام لإقرار الثقة في الامتدادات الأمنية لنظام اسم النطاق DNSSEC. ولدعم التحقق من موثوقية أنواع عدة من التوقيعات الرقمية والتي يتم نشرها على الموقع المخصص ذاته، وبصيغة OpenPGP وPKCS#7 وشهادة X.509 تحتوي على مفتاح الجذر.

على الرغم من أهمية تحديد الموثوقية للغاية، فإنه يجري إغفاله في الغالب ويكون منخفض التحديد كذلك. وعندما تم توفير الإجراءات لدعم براهين الموثوقية للحصول على مراجعة العامة، فقد كان هناك تعليقات موضوعية ذات حجم منخفض. حيث يقوّض هذا الجهود المبذولة لدعم الموثوقية بشكل كافي. ويبدو من الممكن بأن المراجعة الإضافية (مع تغييرات توافق التراجع، حسب الاقتضاء) مستحقة. وكما ذكر من قبل، فإنه يدعم فريق التصميم مناقشة المجتمع ومراجعته لمسودة الإنترنت تحت عنوان "نشر مرتكز ثقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC" (سبق وردها) ضمن فريق عمل هندسة الإنترنت IETF، مع هدف نشر مواصفة ثابتة قائمة على مراجعة الأقران في مجموعة طلب الحصول على التعليقات RFC.

ويقترح دعم الاسترجاعات المراقبة للتوقيعات الرقمية موثوقة الدعم بأنه قلة من الأطراف المعتمدة، إن وجد، قد استفادت من التوقيعات الرقمية. حيث لا تكتسب الثقة بسهولة عبر تقديم التوقيعات الرقمية، إلا أنه ينبثق من الترويج الفعال.

التوصية 4: ينبغي على ICANN إتخاذ دور فعّال في تعزيز مصادقة مرتكز الثقة في منطقة الجذر، بما فيها تسليط الضوء على المعلومات المنشورة في موقع IANA الخاص بـ ICANN.

6.3 التأثير على إدارة مفتاح الدخول الرئيسي KSK لمنطقة الجذر

وكما هو موضح في بيان ممارسة الامتدادات الأمنية لنظام اسم النطاق DNSSEC لمشغل مفتاح الدخول الرئيسي KSK لمنطقة الجذر، يسجل مشغل مفتاح الدخول الرئيسي KSK لمنطقة الجذر كل قمة DNSKEY RRsets الخاصة بمنطقة الجذر عبر طريقة طلب تسجيل المفتاح KSR الذي يقدمه مشغل مفتاح تسجيل منطقة الجذر ZSK لمنطقة الجذر. وتكوين النتيجة رد المفتاح الموقع والذي يتكون من مجموعة من DNSKEY RRsets الموقعة مقدمة لمشرف منطقة الجذر.

ويتم توثيق هذه العمليات جيداً وفي حالة الإجراءات التي تجري خلال مراسم مفتاح الدخول الرئيسي KSK، والذي يخضع للتدقيق الخارجي والمراقبة واسعة النطاق؛ حيث يعتبره فريق التصميم مفيد للغاية لتجنب أية تغييرات موضوعية للعمليات كنتيجة لتغيير مفتاح الدخول الرئيسي KSK وذلك لتفادي تعطيل العملية التي تعتبر مفهومة بشكل جيد فعلياً في نموذجها الحالي.

[16] مدرجة في https://www.iana.org/dnssec/files

التوصية 5: ينبغي ألا يتطلب تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر تغييرات جوهرية على العملية الحالية من أجل إبقاء مستويات عالية من الشفافية المرتبطة بها.

ويشتمل كل طلب تسجيل مفتاح KSR دورة زمنية لربع تقويمي واحد (ثلاثة أشهر أو ما يقارب 90 يوم) ويتم تقييمها إلى 9 فترات زمنية من 10 أيام لكل منها. إذا كانت الدورة الزمنية أكثر من 90 يوم، يتم تمديد الفترة الزمنية الأخيرة في الدورة لتعبئة الفترة. ونتيجة لهذا، يجب أن تتماشى كافة التغييرات على DNSKEY RRset لمنطقة الجذر، مثلاً، إضافة و/أو إزالة المفاتيح كما هو مطلوب حسب تغيير المفتاح مع هذه الفترات الزمنية لمدة 10 أيام لتخفيف أية تغييرات موضوعية في العمليات المستخدمة لنشر منطقة الجذر الموقعة.

التوصية 6: ينبغي أن تتماشى كافة تغييرات مجموعات سجل المورد لمفتاح نظام اسم النطاق DNSKEY في منطقة الجذر مع فترات زمنية لمدة 10 أيام واردة في بيان ممارس DNSSEC لمشغلات مفتاح الدخول الرئيسي KSK.

ومع الفترات المعيارية، يزداد حجم رد مجموعة DNSKEY RRset للجذر مع أول وآخر فترة في كل دورة زمنية. تتألف الفترة الأولى لما بعد نشر مفتاح تسجيل منطقة الجذر ZSK من الدورة الزمنية السابقة، بينما تتألف الفترة الأخيرة لما قبل النشر للدورة الزمنية التالية.

ولتحفيف القضايا المحتملة والمرتبطة بأحجام ردود نظام اسم النطاق DNS الأكبر، فمن المستحسن جدولة التغيير بحيث من الممكن المحافظة على حجم رد DNSKEY RRset بأصغر قدر ممكن. ويظهر إجراء فحص مفصل لقضايا حجم الرد مع التوصيات المرافقة في هذه الوثيقة لاحقاً. وتم إدراج جدول تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر والمصمم مع مراعات الاعتبارات المذكورة أعلاه أيضاً في هذه الوثيقة لاحقاً.

6.4 اعتبارات التشفير

نظر فريق التصميم في سؤال ما إذا كان هناك أسس مقنعة بما يكفي للنظر في التغيير في حجم المفتاح أو الخوارزمية بالنسبة لمفتاح الدخول الرئيسي KSK. وقد ينشأ الأساس المقنع من أسئلة متعلقة بقوة التشفير في حجم المفتاح أو الخوارزمية المختار.

وقد أعلن القصد من رفع الحد الأدنى من نقاط قوة التشفير، وذلك مع النشر الأولي لـ SP 800-57، للجزء رقم واحد (توصيات لإدارة المفتاح) في عام 2005. إلا أنه وفي السنوات الخمس فيما بين النشر والتاريخ النهائي المقترح، لم يحرز تحليل الوسائل التقنية تقدماً بأسرع قدر ممكن كما هو متوقع. لا يوجد لاقتراح أنه ثمة ضرورة ملحة لاستخدام أطوال مفتاح أكثر طولاً لمفتاح الدخول الرئيسي KSK لمنطقة الجذر.

6.4.1 تشفير الحقل المحدود

يعتبر عدم تشابه البت 2048 لمفتاح RSA مساوي لتشابه مفتاح بتات 103 في التقرير السنوي 2012 لـ ECRYPT II حول الخوارزميات وأحجام المفتاح[17]. ويوصي التقرير ذاته باستخدام 96 جزء من الأمان على الأقل لحماية مدتها 10 سنوات. توصيات المعهد الوطني للمعايير والتكنولوجيا (NIST) لإدارة المفتاح - الجزء 1: تنظر (المراجعة 3) العامة[18] في تساوي مفتاح RSA البت 2048 من بتات 112 للأمان وتعتبر هذه القوة مقبولة للاستخدام في المدة من 2014 إلى 2030. وينظر The French Agence nationale de la sécurité des

[17] http://www.ecrypt.eu.org/ecrypt2/documents/D.SPA.20.pdf
[18] http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf

systèmes d'information (ANSSI) Référentiel Général de Sécurité[19] كذلك في مفتاح RSA الجزء 2048 ليغدو آمناً للاستخدام حتى عام 2030.

يدوم المحتوى الموقع في منطقة الجذر عادة حيث تقاس فترات توقيع DNSKEY في أيام (15 يوم)، ويعتقد فريق التصميم بأنه ينبغي أن يكون مفتاح RSA جزء 2048 آمن لمزيد من خمس سنوات ما لم يكن هناك اختراق تكنولوجي عام في جانب تحليل عوامل عدد صحيح كبير.

6.4.2 تشفير منحنى إهليليجي

يعتبر خيار الخوارزمية الأخرى المتوفرة للامتدادات الأمنية لنظام اسم النطاق DNSSEC خوارزمية توقيع رقمي ذو منحنى إهليليجي (ECDSA) والمحدد في RFC 6605[20]. تحتوي خوارزمية توقيع رقمي ذو منحنى إهليليجي ECDSA خصائص والذي يجعل الأمر مرغوب لاستخدامه كخوارزمية لمفتاح الدخول الرئيسي لمنطقة الجذر. وتعتبر المفاتيح أصغر بكثير مع الإبقاء على قوة معادلة لمفاتيح RSA. وتتمثل التقديرات الحالية في احتواء خوارزمية توقيع رقمي ذو منحنى إهليليجي ECDSA مع المنحنى P -256 قوة معادلة لـ RSA مع مفاتيح من 3072 بت المعهد الوطني للمعايير والتكنولوجيا (NIST) أو 3248 بت (ECRYPT II). إلا أنه تم توحيد الخوارزمية لاستخدامها في الامتدادات الأمنية لنظام اسم النطاق DNSSEC في الآونة الأخيرة نسبياً فقط - تم نشر RFC 6605 في عام 2012 - وقد راقبت التدابير التي وردت لاحقاً في هذه الوثيقة بأن دعم خوارزمية توقيع رقمي ذو منحنى إهليليجي ECDSA في المحققات ليس بقدر واسع النطاق كما دعم RSA (راجع القسم - الاعتبارات التشغيلية).

كما وتعمل مجموعة بحث منتدى تشفير فريق عمل هندسة الإنترنت IETF (CFRG) على طلب جديد للحصول على التعليقات RFC "منحنى إهليليجي للأمان" حيث يضيف أمان منحنيات إهليليجية جديدة، كما تعرب عن بعض المخاوف من مجتمع التشفير حول الإنشاء ونقاط الضعف المحتملة للمنحنيات المستخدمة من خلال خوارزمية توقيع رقمي ذو منحنى إهليليجي ECDSA. ومن المستحسن السماح لمجموعة بحث منتدى تشفير فريق عمل هندسة الإنترنت IETF (CFRG) إكمال عملها على الوثيقة قبل التحول إلى خوارزمية منحنى إهليليجي جديد لتوقيع على منطقة الجذر.

6.4.3 الخلاصة

وجد فريق التصميم وذلك استناداً على التوجيه المذكور أعلاه بأنه لا توجد ضرورة ملحة لتغيير إما الخوارزمية أو حجم مفتاح الدخول الرئيسي KSK من RSA بت 2048. وكما استفاد فريق التصميم من تنفيذ محلل مصادقة نظام اسم النطاق DNS والذي يتطلب من منطقة الجذر للتوقيع من خلال كافة الخوارزميات التي تطابق تهيئة مرتكزات الثقة وبالتالي سوف يتطلب التغيير إلى خوارزمية مختلفة نهج مختلف أكثر من تغيير مفتاح الدخول الرئيسي KSK. ويوفر هذا مزيداً من الدافع العملي لتفادي التغير الحاصل في الخوارزمية في هذا الوقت. وقد تواصل فريق التصميم مع المورد فيما يتعلق بالقضية ومتطلبات المورد، وثمة توقع بأنها ستكون بمثابة تغييرات لمفتاح تسجيل الرئيسي KSK مخففة غير مجدولة مستقبلاً.

وبالنسبة لهذه الأسباب، ينبغي أن يكون مفتاح الدخول الرئيسي KSK المقبل لأول تغيير مفتاح تسجيل رئيسي KSK مفتاح RSA من 2048 بت، إلا أنه قد تكون التغييرات الحاصلة في الخوارزمية و/أو طول المفتاح من الجدير النظر به بخصوص تغييرات مفتاح الدخول الرئيسي KSK التالي.

التوصية 7: يوصي فريق التصميم الاحتفاظ بالخوارزمية الحالية وحجم المفتاح بالنسبة لمفتاح الدخول الرئيسي KSK المقبل فيما يخص تغيير أول مفتاح الدخول الرئيسي KSK لمنطقة الجذر.

[19] http://www.ssi.gouv.fr/uploads/2015/01/RGS_v-2-0_B1.pdf
[20] https://tools.ietf.org/html/rfc6605

التوصية 8: ينبغي مراجعة خيار الخوارزمية وحجم المفتاح في المستقبل بالنسبة لتغييرات مفتاح الدخول الرئيسي KSK لمنطقة الجذر التالية.

6.5 التنسيق والاتصال

6.5.1 التنسيق مع المجتمع التقني وشركاء القناة

ينبغي على ICANN تصميم وتنفيذ خطة الاتصالات وذلك للتوعية بتغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر. لا بد من زيادة الوعي داخل المنتديات التقنة كما تلك حيث تم تقديم التوزيع الأصلي للامتدادات الأمنية لنظام اسم النطاق DNSSEC في منطقة الجذر.

ويشير مصطلح "شركاء القناة" المقبل إلى المنظمات الخارجية التي تيسر استخدام امتدادات أمنية لنظام اسم النطاق DNSSEC مستقلة عن إدارة منقطة الجذر. يشكل شركاء "القناة" هؤلاء قيمة تسجيل خروج منطقة الجذر من شركاء إدارة ملفات منطقة الجذر RZM إلى شبكة الإنترنت العامة العالمية.

ويتم تقسيم شركاء القناة إلى ثلاثة جوانب عامة. الأولى هي العوامل المساعدة، تلك التي تنفيذ برمجيات تحقق الامتدادات الأمنية لنظام اسم النطاق DNSSEC المعنيين بتنفيذ RFC 5011 من بين بنود أخرى. الثاني هو موزعي البرمجيات والأنظمة التي تتضمن برمجيات تحقق الامتدادات الأمنية لنظام اسم النطاق DNSSEC، والمعنين بالأساس مع توزيع نسخ مفتاح الدخول الرئيسي KSK لمنطقة الجذر. الثالثة هي مشغلات أنظمة تحقق الامتدادات الأمنية لنظام اسم النطاق DNSSEC حيث تستفيد من مفتاح الدخول الرئيسي KSK لمنطقة الجذر.

ويوصي فريق التصميم من أجل تيسير الاتصال بأنه ينبغي لكل شريك قناة إبقاء العقد في الملف، إن رغب، وسيتم تقديم تحديثات على تغيير مفتاح الدخول الرئيسي KSK لهذه العقود. ولا يقصد من قائمة العقد هذه بأن يكون حصرياً أو لتبادل المادة الغير متوفرة للجمهور. يقصد من قائمة العقد السماح لأخذ عينات من خطوات التوعية في تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر. إلا أنه ينبغي إبقاء القائمة مغلقة للسماح بشركاء القناة لإدارة التوعية بمعلومات عقودهم المحددة.

التوصية 9: ينبغي على ICANN وبالتعاون مع شركاء إدارة ملفات منطقة الجذر تصميم وتنفيذ خطة الاتصالات لزيادة الوعي بتغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر، بما فيها التواصل مع المجتمع التقني العالمي من خلال اجتماعات تقنية مناسبة ومع "شركاء القناة" كما أولئك الواردين في هذه الوثيقة.

6.5.2 التنسيق مع مشغلات خادم الجذر

يحتوي أي تغيير هيكلي على محتوى منطقة الجذر إحتمالية التأثير على السلوك التشغيلي لخوادم الجذر الفردية. يعتبر الإمداد الأولي للصاق عنوان الاصدار السادس من بروتوكول الانترنت IPv6 (AAA) في منطقة الجذر وتوزيع الامتدادات الأمنية لنظام اسم النطاق DNSSEC اللاحق بمثابة أمثلة للتغييرات التي أجريت بالتشاور والتشاور مع مشغلات خادم الجذر عن كثب، بما أنه قد تسببت هذه التغييرات بإحداث تغيير على أنماط الاستفسار. وبالتالي يملي الحذر مع البنية التحتية الهامة نهجاً محافظاً لأي تغيير حاصل في حالة حدوث عواقب غير متوقعة والتي تؤدي إلى تدهور أداء نظام خادم ملف الجذر بأكمله.

حيث تشير التجربة التي أجريت كجزء من تحضير هذه الوثيقة بأنه لن يترتب عن حالة تغيير مفتاح الدخول الرئيسي KSK أية أضرار؛ إلا أنه يوصى بنهج محافظ كما مع الأمثلة السابقة للتغيير الهيكلي المذكور أعلاه.

ويقترح فريق التصميم بأنه لربما تتعامل مشغلات خادم الجذر الفردي مع أحداث معينة ضمن فترة تغيير مفتاح الدخول الرئيسي KSK حيث من شأنها أن تتعامل مع الحدث التشغيلي المخطط ذو الأهمية بإصدار إشعارات حالة عامة والتنسيق مع مشغلات خوادم الجذر الأخرى وذلك باستخدام قنوات حقيقية اعتيادية مستخدمة لهذا النوع من الأحداث. وينبغي أن تدرج هذه الأحداث الفترة المحيطة بإضافة مفتاح تسجيل رئيسي KSK جديد مقبل إلى قمة DNSKEY RRSet لمنطقة الجذر، وإزالة مفتاح الدخول الرئيسي KSK الجاري من RRset ذاتها.

ويقترح فريق التصميم بأن تمارس قنوات الاتصالات الحقيقية بين مشغلات خادم الجذر الفردي وICANN وما بين ICANN وشركاء إدارة ملفات منطقة الجذر RZM الأخرى على نحو مشابه حول الأحداث ذاتها لضمان تحديد أي تأثير متوقع ومشاركته فوراً.

وينبغي مراجعة الجدول الزمني المفصّل لفترة تغيير مفتاح الدخول الرئيسي KSK عبر مشغلات خوادم الجذر قبل استكمالها ونشرها، وذلك من أجل التأكد من أنها لا تتعارض مع أي من الخطط الأخرى التي قد تحد من قدر مشغل خادم الجذر الفردي لتقديم مستوى مقبول من التغطية التشغيلية. وينبغي بذل جهد لتعديل توقيت التغيير لتفادي التعارض التشغيل، بقدر ما هو عملي.

التوصية 10: ينبغي على ICANN أن تطلب من اللجنة الاستشارية لنظام خادم الجذر RSSAC تنسيق مراجعة بالجدول الزمني المفصل بالنسبة لمدة تغيير مفتاح تسجيل الدخول KSK قبل أن يتم نشرها، وينبغي احتواء الطلبات المعقولة لتعديل ذلك الجدول الزمني في الحدث بحيث يحدد أي مشغل خادم جذر أسباب تشغيلية للقيام بذلك.

التوصية 11: ينبغي على ICANN التعاون مع اللجنة الاستشارية لنظام خادم الجذر RSSAC وشركاء إدارة ملفات منطقة الجذر RZM لضمان استخدام قنوات الاتصالات في الوقت الحقيقي وذلك للتأكد من الوعي التشغيلي المناسب بنظام خادم ملف الجذر لكل تغيير حاصل في منطقة الجذر والذي يتضمن إضافة أو إزالة مفتاح الدخول الرئيسي.

يتم تيسير فهم التأثير التشغيلي لتغيير مفتاح الدخول الرئيسي KSK على المحققات وخوادم الجذر ذاتها عبر مجموعة البيانات من خلال مشعلات خادم الجذر على مدار تغيير مفتاح الدخول الرئيسي KSK. وبما أن نظام خادم الجذر متنوع سواء في البنية أو توزيعها في جميع أنحاء الإنترنت، فمن المفهوم أنه سوف تتضمن الفرص لمجموعة البيانات القائمة على توقيت طويل عبر مشغلات خادم الجذر الفردي قيوداً متنوعة حيث من الصعب تمييزها باختصار مفيد للنظام بأكمله. ومن المفهوم كذلك أنه توجد إمكانيات تجميع البيانات الأساسية بالفعل وذلك لإرضاء المتطلبات التكتيكية لمراقبة شروط الخدمة في الوقت الحقيقي، بينما يحرز تغيير مفتاح الدخول الرئيسي KSK تقدماً.

وعندما تم توزيع الامتدادات الأمنية لنظام اسم النطاق DNSSEC بداية في منطقة الجذر، حيث جرى تنفيذ ممارسة تجميع البيانات الكبيرة، حيث أثبتت البيانات الناتجة فائدة التحليل دون الاتصال بالإنترنت لرد فعل نظام اسم النطاق DNS بأكمله لإجراء تغييرات هيكلية جارية في منطقة الجذر، بما فيها تحليل الأطراف الثالثة، وبتسهيل من مركز الأبحاث والتحليل والعمليات لنظام اسم النطاق DNS-OARC[21]. ويتم ضمان تدريب مشابه لتغيير أول مفتاح تسجيل رئيسي.

التوصية 12: ينبغي على ICANN التعاون مع اللجنة الاستشارية لنظام خادم الجذر RSSAC لطلب تنفيذ مشغلات خادم الجذر مجموعة البيانات حيث ستبلغ عن التحليل التالي وتساعد في وصف التأثير التشغيلي المترتب على تغيير مفتاح الدخول الرئيسي، وبأنه يجب توفير الخطط والمنتجات لمجموعة البيانات تلك وذلك للحصول على تحليل الطرف الثالث.

[21] https://www.dns-oarc.net

6.5.3 التنسيق بين مشغل مفتاح الدخول الرئيسي KSK ومشغل مفتاح تسجيل منطقة الجذر

يتم تكليف مسؤولية إدارة مفتاح الدخول الرئيسي KSK لمنطقة الجذر ومفتاح تسجيل منطقة الجذر ZSK بشكل منفصل إلى مشغل وظائف IANA ومشرف منطقة الجذر على التوالي. وتتم إدارة الدورين بشكل منفصل.

ويعتبر مفتاح تسجيل منطقة الجذر ZSK لمنطقة الجذر حالياً هو مفتاح من RSA 1024 بت، كما هو محدد في بيان ممارسات الامتدادات الأمنية لنظام اسم النطاق DNSSEC الخاص بمشرف مفتاح تسجيل منطقة الجذر[22]. فمن المحتمل أن يزيد مشرف منطقة الجذر من حجم المفتاح لمفتاح تسجيل منطقة الجذر ZSK في المستقبل.

ويتم تغيير مفتاح تسجيل منطقة الجذر ZSK بشكل منتظم حسب الجدول لمدة 90 يوم، ومن المتوقع أن يستمر هذا كالمعتاد أثناء فترة تغيير مفتاح الدخول الرئيسي KSK؛ بما أنه من المتوقع أن تمتد فترة تغيير مفتاح الدخول الرئيسي KSK لأكثر من 90 يوم، وسيكون هناك فترات خلالها حيث تتألف قمة DNSKEY RRSet لمنطقة الجذر من أربعة مفاتيح بناءً على الخطة النهائية.

وقد تؤدي زيادة حجم مفتاح تسجيل منطقة الجذر أثناء تغيير المفتاح إلى سلوك مختلف لدى المدققين بالنسبة لجزء فترة تغيير مفتاح الدخول الرئيسي KSK، بما أنه ستزداد أحجام الرد مع حجم مفتاح تسجيل منطقة الجذر ZSK. وقد يعقد هذا الأمر الجهود المبذولة لتحديد وفهم وتخفيف أي من المشاكل التشغيلية البارزة.

ويكون أي قرار مرتبط بحجم مفتاح تسجيل منطقة الجذر ZSK خارج نطاق هذه الوثيقة. إلا أننا نوصي بتنسيق ICANN مع مشرف منطقة الجذر وذلك لضمان تنسيق أي زيادة في حجم مفتاح تسجيل منطقة الجذر ZSK مستقبلاً بدقة مع استبدالات مفتاح الدخول الرئيسي KSK، كأن لا يتم تنفيذ التدريبين في الوقت ذاته.

التوصية 13: ينبغي على شركاء إدارة ملفات منطقة الجذر RZM ضمان تنسيق أية زيادة مستقبلية في حجم مفتاح تسجيل الجذر ZSK بدقة مع مغيري مفتاح الدخول الرئيسي، كأن لا يتم تنفيذ العملتين بشكل متزامن.

7 التأثير على مصادقة المحللات

7.1 اعتبارات حجم الحزمة

يتم تحديد نظام اسم النطاق DNS للعمل على بروتوكول مخطط المستخدم UDP وبروتوكولات نقل بروتوكول التحكم بالإرسال TCP. تم تفضيل بروتوكول مخطط المستخدم UDP في بروتوكول نظام اسم النطاق DNS نظراً لانخفاض النفقات العامة في بروتوكول مخطط المستخدم UDP لدى مقارنتها ببروتوكول التحكم بالإرسال TCP، ولا سيما من حيث الحفاظ على حالات الربط على الخادم. إلا أنه يوجد قيد يفرضه خيار هذا البروتوكول. فقد اقتصرت ردود بروتوكول مخطط المستخدم UDP في التعريف الأصلي لنظام اسم النطاق DNS RFC 1035على مجموعة ثمانية. ولا زالت تجري مراقبة قيد ثمانية 512 في البرمجيات حتى اليوم، إما بتكريم أو تطبيق ذلك القيد.

ومن خلال آلية التمديد لنظام اسم النطاق EDNS(0)، DNS، والتي تم تحديدها أصلاً في طلب الحصول على التعليقات RFC المنشورة في شهر أغسطس، 1999 [RFC 2671]، يتمكن طالب نظام اسم النطاق DNS بتحديث عبر RFC 6891] من إبلاغ خادم نظام اسم النطاق DNS حيث يتمكن من التعامل مع أحجام رد بروتوكول مخطط المستخدم UDP أطول من مجموعة ثمانية 512. ويضع مقدم الطلب الحد الأقصى من حجم حمولة بروتوكول مخطط المستخدم UDP (ليس حجم حزمة بروتوكول الإنترنت IP بل حجم رسالة نظام اسم النطاق DNS) في الاستفسار،

[22] http://www.verisigninc.com/assets/dps-zsk-operator-1527.pdf

ويطلب الخادم للاستجابة مع رد بروتوكول مخطط المستخدم UDP حيث لا يكون حجم حمولة نظام اسم النطاق DNS أكبر من حجم المخزن المؤقت. وإن لم يكن هذا ممكناً، يحدد الخادم حينها اقتطاع البت رداً على الإشارة إلى حدوث الاقتطاع. وإذا تضمن الرد المقتطع رسالة نظام اسم نطاق DNS صحيحة، فقد يختار مقدم الطلب استخدام الرد المقتطع. أو يعمل مقدم الطلب على فتح جلسة بروتوكول التحكم بالإرسال للخادم ويكرر الاستفسار عبر بروتوكول التحكم بالإرسال TCP.

ولا بد من إشارة أنظمة نظام اسم النطاق DNS التي تستفيد من الامتدادات الأمنية لنظام اسم النطاق DNSSEC إلى قدرتهم على القيام بالأمر وذلك باستخدام علامة DO (DNSSEC OK) في شبه عنوان EDNS. وبما أنه يتعلق التأثير التشغيلي المراعاة في هذه الوثيقة بالكامل بالأنظمة التي تعد قادرة على الامتدادات الأمنية لنظام اسم النطاق DNSSEC، تعتبر الأنظمة المعنية قادرة على EDNS(0) (وذلك لأنه تتطلب الامتددادات الأمنية لنظام اسم النطاق DNSSEC دعم EDNS(0) support) وبالتالي لا يقتصر على قيد مجموعة ثمانية 512.

وقد باشر العميل المعاملة في بروتوكول التحكم بالإرسال TCP، إلا أن سلوك مقدم الطلب العادي على وشك بدء المعاملة في بروتوكول مخطط المستخدم UDP، واستخدام البت المقتطع رداً على الإشارة بأنه ينبغي على مقدم الطلب استخدام بروتوكول التحكم بالإرسال TCP للاستفسار.

ويتم التعامل مع تجزئة حزمة بروتوكول مخطط المستخدم UDP بشكل مختلف في الاصدار الرابع من بروتوكول الانترنت IPv4 والاصدار السادس من بروتوكول الانترنت IPv6. وعندما تكون الحزمة كبيرة للغاية بالنسبة لوسط إرسال حزمة بروتوكول الإنترنت IP الأساسية، فقد تتم تجزئة حزمة بروتوكول الإنترنت IP. وتستخدم الأجزاء الزائدة في هذه الحالة دليل مستوى بروتوكول الإنترنت IP ذاته (بما فيها حقل رقم البروتوكول لبروتوكول مخطط المستخدم (UDP، إلا أنها تستثني بالتحديد شبه عنوان بروتوكول مخطط المستخدم UDP في الأجزاء الزائدة. وقد تجزء حزمة بروتوكول الإنترنت IP في الاصدار الرابع من بروتوكول الإنترنت IPv4، المرسل الأصلي أو أي موجه مباشر، ما لم يتم تحديد علامة بروتوكول الإنترنت IP عدم التجزئة. وقد تجزء حزمة بروتوكول الإنترنت IP في الاصدار السادس من بروتوكول الانترنت IPv6 فقط المرسل الأصلي. وإن لم يتمكن الموجه المباشر من إحالة الحزمة إلى واجهة الوصلة التالية حينها في الاصدار السادس من بروتوكول الانترنت IPv6، سيولد الموجه حزمة تشخيص ICMPv6 مع حجم وحدة الإنتقال القصوى MTU في واجهة الوصلة التالية والدور الرئيسي للحزمة، وتمرير هذه المعلومات إلى مرسل الحزمة.

ولدى استخدام بروتوكول مخطط المستخدم UDP، لا يحتفظ المرسل بمخزن مؤقت من البيانات الغير معترف بها، وبالتالي لا يتمكن مرسل الاصدار السادس من بروتوكول الانترنت IPv6 لدى تلقي هذه الرسالة من إعادة إرسال البيانات الأصلية. وتظهر البيانات التجريبية لاقتراح أن الرد العادي من عمليات تنفيذ عديدة من الاصدار السادس من بروتوكول الانترنت IPv6 لإنشاء مدخل المضيف في قائمة إحالة الاصدار السادس من بروتوكول الانترنت IPv6 المحلي، وتسجيل وحدة الإنتقال القصوى MTU الواردة في هذه القائمة لمدة التخزين المؤقت المحددة محلياً. ويعني هذا بأنه سوف تستخدم أية محاولات لاحقة لإرسال حزمة بروتوكول مخطط المستخدم UDP للاصدار السادس من بروتوكول الانترنت IPv6 إلى هذه الوجهة قيمة وحدة الإنتقال القصوى MTU هذه لتحديد طريقة تجزئة الحزمة الجارية.

7.1.1 تجربة القياس

وهي تجربة تم تصميمها وإعدادها لإنتاج بيئة لحالة خادم الجذر وذلك من أجل تقييم ما التأثير الذي يحدثه حجم الحزمة الكبيرة على المحللات والمستخدمين.

وقد تتحقق هذا باستخدام برنامج إعلان عبر الإنترنت لتشجيع محللات نظام اسم النطاق على طرح استفسارات فريدة من نوعها إلى اسم خادم موثوق مهيئ للرد على الاستفسارات لمنطقتين بأحجام رد مختلف. ويعتقد بأن المحللات التي تطرح الاستفسارات على اسم الخادم الموثوق في هذه الاختبارات هي نفس مجموعة المحللات إلى حد كبير والذي من المتوقع منهم الاستفسار عن منطقة الجذر.

ولإجراء اختبار فيما إذا كان قد تلقى المحلل رد كبير على الإعلان المستفسر عنه فيما يخص اسم النطاق المستهدف. وسيقوم اسم النطاق المستهدف بذاته على إعادة رد ما بحجم طبيعي. إلا أنه ومن أجل الوصول إلى الرد المستهدف، كان لا بد من تلقي المحلل رد مباشر كبير بدايةً. وإذا نجح المحلل في طلب الحصول على معلومات اسم النطاق المستهدف، فقد أظهر الاختبار حينها بأنه من الممكن أن يتعامل المحلل مع الرد الكبير المباشر.

وتضمن الاختبار كذلك استرجاع موضوع ويب من تجربة خادم الويب، وذلك بالسماح للتجربة مطابقة العناوين المستخدمة في استرجاع الويب (عنوان IP للمستخدم النهائي) لعناوين مستخدمة من خلال محللات الاسم في طرح استفسار نظام اسم النطاق DNS.

وقد تم استخدام رد نظام اسم النطاق DNS ثماني 1,444 في هذا الاختبار.

7.1.2 نتائج الاختبار

جلب ما يقارب 7.26 مليون نظام نهائي في مدة خمس أيام خلال شهر مايو 2015 سجل تحكم صغير بنجاح، وجلبت من هؤلاء ما يقارب 7.17 مليون نظام سجل الاختبار بنجاح، بفارق حوالي 90,000 من المستخدمين، أو 1% من مجموعة العينة، والتي فشلت في جلت سجل اختبار نظام اسم النطاق DNS الثماني 1,444.

واستخدمت هذه الأنظمة النهائية ما يقارب 83,000 عناوين IP مختلفة من محلل نظام اسم النطاق DNS. وقد حصل من هؤلاء 94% من المحللين على كل من سجل التحكم وسجل الاختبار بنجاح. ومن 4,251 ممن استرجعوا سجل التحكم إلا أنهم فشلوا في استرجاع سجل الاختبار، فقد استخدام 3,396 امتداد EDNS(0) مع مجموعة بت موافقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC والتي أدت إلى رد مجموعة ثمانية 1,444. وقد تمت مراقبة 3,110 محلل من بين المحللات الفاشلة مرة واحدة فقط خلال التجربة، بينما أظهر 826 محلل حالة الفشل أكثر من مرة. ويعني هذا بأنه فشل 1% من المحللات التي شوهدت في هذه التجربة باسترجاع رد كبير مرتين أو أكثر، بينما شوهد أيضاً 3% من المحللات التي فشلت في استرجاع الرد الكبير مرة واحدة فقط، وهو أمر غير كافي للاختتام بأي تأكيد بأنهم سيفشلون مع الردود الكبيرة باستمرار. واستخدم أقل من 3,000 نظام نهائي قليلاً ما نسبته 1% من هذه المحللات التي فشلت مرتين أو أكثر باستمرار، أو 0.04% من عينات كثافة النظام النهائي.

استخدم ما يقارب 5,237 من المحللات عناوين الاصدار السادس من بروتوكول الانترنت IPv6 في هذا الاختبار (6% من المجموع) بينما فشل 830 من هؤلاء المحللات في استرجاع سجل الاختبار (21% من المحللات الفاشلة). حيث تقترح هذه البيانات قضية محتملة مع بعض محللات الاصدار السادس من بروتوكول الانترنت IPv6 وتعاملها مع أحجام وحدة الإنتقال القصوى MTU.

ومن حيث قياس التغير في حمل الاستفسار مع الردود الكبيرة، فقد تم الاستفسار عن اسم التحكم (مع حجم رد ثماني 93) 16.4 مليون مرة، وجرت مراقبة 475 استفسار باستخدام بروتوكول التحكم بالإرسال TCP. وتم الاستفسار عن اسم

الاختبار (مع حجم رد ثماني 1,444) 18.6 مليون مرة، وتم تقديم 1.2 مليون من هذه الاستفسارات عبر بروتوكول التحمن بالإرسال، أو ما يقارب 6.5% من مجموع عدد الاستفسار لاسم الاختبار. حيث يوجد فرق في مجموع عدد الاستفسارات المقدمة لسجل التحكم مقابل مجموع عدد الاستفسارات لسجل الاختبار. ومن الممكن توضيح الفرق من خلال المحللات رداً على الردود المقتطعة الواردة لسجل الاختبار وذلك عبر إرسال استفسار آخر عبر بروتوكول التحكم بالإرسال TCP. وترتبط النتيجة بشكل معقول مع توزيع أحجام ذاكرة بروتوكول مخطط المستخدم UDP المطروحة في امتدادات EDNS(0) من استفسارات بروتوكول مخطط المستخدم UDP. وقد يتوقع الخادم الموثوق لدى تلقي ردود أكبر حمل استفسار أعلى، ونسبة استفسارات أعلى عبر بروتوكول التحكم بالإرسال TCP.

7.1.3 الخلاصة

ويبدو عدم قدرة ما يقارب 10% من محللات نظام اسم النطاق DNS حيث تحدد علامة موافقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC في استفساراتها من تلقي رد نظام اسم النطاق DNS من مجموعة ثمانية 1,444 (تعني العوامل التجريبية المجهولة بأن الحد الأعلى من هذا العدد هو 6% من كافة المحللات). ومن ضمن هذه المجموعة من المحللات، يتم تمثيل المحللات التي تستخدم الاصدار السادس من بروتوكول الانترنت IPv6 باعتبارها بروتوكول نقل بشكل غير مناسب. فمن المحتمل أن يعود معدل هذا الفشل إلى وجود أشكال متنوعة من برمجيات وسيطة معترضة لنظام اسم النطاق DNS، أو في حالة الاصدار السادس من بروتوكول الانترنت IPv6 نظراً لسوء التعامل المحتمل للرسائل ذات حزم ICMP6 الكبيرة للغاية، إلا أنه لا يمكن إنشاء الطبيعة الدقيقة لحالات الفشل من خلال هذه المنهجية التجريبية.

وتمثل المحللات التي فشلت في تلقي الردود نسبة ضئيلة جداً من المستخدمين. ويبدو أن نسبة عدد المستخدمين الذين يستخدمون محللات نظام اسم النطاق DNS الغير قادرين على حل اسم نظام اسم النطاق DNS باستمرار عندما يشارك ردود نظام اسم النطاق DNS في هذا الحجم 0.04% من كافة المستخدمين (تعني العوامل التجريبية المجهولة أن الحد الأعلى من هذا العدد هو 1% من كافة المستخدمين).

واختبرت هذه التجارب رد نظام اسم نطاق DNS من مجموعة ثمانية 1,444. فمن الملاحظ أنه تقدم أجزاء أخرى من نظام اسم النطاق DNS فعلياً ردود أكبر بشكل ملحوظ من الحجم الذي يجري بحثه هنا ولا يبدو أنه قد أنشأت أحجام الرد هذه على انتباه العامة أو التعليقات الواضحة. على سبيل المثال، فقد أنشأ استفسار DNSKEY المماثل لاسم org. في السادس من يونيو 2015 رد مجموعة ثمانية 1,625 والذي يتألف من مفاتيحي تسجيل رئيسية من RSA 2048 بت، ومفاتيحي تسجيل المنطقة RSA من 1024 بت وثلاثة تواقيع - واحدة من مفتاح الدخول الرئيسي وأخرى من مفاتيح تسجيل المنطقة. ولن تتمكن المحللات المصادقة غير القادرة على تلقي هذا النوع من ردود نظام اسم النطاق DNS الكبيرة من مصادقة توقيع إما سجل DS أو سجل NSEC3 (والتي تستخدم للإشارة إلى عدم وجود سجل DS) لكل تفويض في منطقة .org، الأمر الذي يتسبب بفشل قرار نظام اسم النطاق DNS للتفويضات في org. بنحو فعال.

ولا يدرك فريق التصميم أي من المشاكل التشغيلية التي قد يواجهها حاملو اسم النطاق في org. فيما يتعلق بحجم حزمة رد نظام اسم النطاق DNS DNSKEY لاسم org. وحتى بعد مراعاة العدد الضئيل للغاية للمناطق المسجلة ضمن org.، يشير الافتقار لأي تقارير تشغيلية فيما يتعلق بفشل القرار في أسماء النطاق org. إلى أنه من غير المرجح تمثيل حجم الرد باعتباره قضية تشغيلية هامة بالنسبة لتغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر.

أما الفرق الواحد للملاحظة بين حالة الاختبار ووضع org. هو أنه سوف تستفسر المحللات التي تجري مصادقة فعلياً فيما يخص DNSKEY RRset الكبير. وفي حالة الاختبار، ستحاول كافة محللات إشارة موافقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC لجلب الرد الكبير. ويبدو الأمر كما هو موصوف في القسم 8.2 بأن أقل من 30% من تحديد المحللات موافقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC في مصادقة برنامج الاستفسار الأصلي للرد لاحقاً. فمن المحتمل بأنه كانت مشغلات المحلل هذه والتي شغلت المصادقة أكثر تفانياً في تحديد وتصحيح أية قضايا

متعلقة بالشبكة والذي قد يمنعها من استرجاع حزم رد كبيرة، حيث ستكون هذه المحللات عرضة لتجربة هذه المشاكل. بينما ستواجه محللات أخرى، دون إجراء المصادقة، حزم رد كبيرة فقط تحت ظروف نادرة نسبياً، وربما لا يدركون هذه القيود المفروضة بموجبهم حسب بيئة شبكاتهم.

ومن المعقول الاستدلال إلى أن الغالبية العظمة من أولئك الذين فشلوا في تلقي الرد الكبير في الاختبارات بمثابة محللات غير مصادقة، والتي لن تتأثر بزيادة حجم سجل مورد DNSKEY لمنطقة الجذر.

وباختصار، تشير هذه الاختبارات إلى أنه قد يتأثر أقل من 0.04% من المستخدمين بحجم الرد الأكبر خلال تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر، إلا أنه بمثابة تقدير بعامل مجهول عالي، حيث تميل الملاحظات المستمدة من TLDs مع مجموعة مفاتيح كبيرة إلى الإشارة بأن هذا بمثابة الحد الأعلى لمدى التأثير من حجم الرد الأكبر.[23]

7.2 سلوك مصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC

توجد ثلاثة جوانب لقياس سلوك مصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC. الجانب الأول هو استرجاع التوقيعات الرقمية للامتدادات الامنية لنظام اسم النطاق DNSSEC (تحديد علامة موافقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC من خيارات (0)EDNS في الاستفسار)، أما الجانب الثاني هو وظيفة المصادقة حيث يتم إنشاء سلسلة الثقة من مفتاح الجذر للاسم الذي يجري مصادقته، والجانب الثالث هو ما إذا كان تهيئة قرار اسم المستخدم سيتقبل فشل مصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC بوصفه فشل نهائي أو فيما لو تمت إحالة الاستفسار إلى محلل آخر.

7.2.1 نتائج الاختبار

جرت مراقبة ما يقارب 85% إلى 90% من المستخدمين في مايو 2015 لتمرير استفساراتهم إلى المحللات باستخدام التجربة الموصوفة أعلاه (القسم 7.1.1) حيث تضمنت الاستفسارات المترتبة لدى اسم خادم موثوق لاسم غير مخزن مؤقتاً خيار (0)EDNS) في الاستفسار وحددت كذلك علامة موافقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC.

فقد أجرت ما يقارب 24% من كثافة عينة المستخدم ذاتها استفسارات لاحقة حيث تبين مصادقة المحلل للرد باستخدام الامتدادات الأمنية لنظام اسم النطاق DNSSEC باتباع سلسلة من التوقيعات التبادلية وذلك بنسخ سلسلة تفويض الاسم الاحتياطي إلى مفتاح الدخول الرئيسي KSK لمنطقة الجذر.

ويتوافق ما يقارب 11% من عينة كثافة المستخدم ذاتها مع سلوك المستخدم النهائي والذي سيتجاوب مع فشل مصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC من المرور السابق عبر تمرير الاستفسار إلى محلل مختلف لا يؤدي مصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC.

ويشير هذا إلى أنه يتمتع أي تغير في إجراءات مصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC بإحتمالية التأثير على ما يقار ربع كثافة مستخدم الإنترنت.

ومن هؤلاء، يفسر أقل من نصف مجموعة المستخدمين فشل مصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC فعلياً (يشار إليها بـ SERVFAIL) كإشارة لتقديم الاستفسار ذاته إلى محلل مختلف لا يجري مصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC. ومن المحتمل أن يتضمن تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر بالنسبة لمجموعة مستخدمي الإنترنت بنسبة 11% مفتاح تسجيل رئيسي KSK لمنطقة الجذر غير معترف به وفشل المصادقة،

[23] ترد المزيد من التفاصيل عن التجربة والنتائج على http://www.potaroo.net/ispcol/2015-05/ksk.html.

إلا أنه قد أظهر هؤلاء المستخدمين بأنهم يفسرون SERVFAIL فعلياً عبر استخدام محلل بديل. ومن المحتمل أن تتضمن النتائج مدة أطول لحل أسماء الامتدادات الأمنية لنظام اسم النطاق DNSSEC المسجلة، إلا أنه لن يؤدي إلى العجز عن حل الاسم إطلاقاً.

ومن المحتمل تعرض 13% من المستخدمين المتبقين ممن لا يعودون إلى محلل غير مصادق عند تلقي رد SERVFAIL لعدم القدرة على حل اسم الامتدادات الأمنية لنظام اسم النطاق DNSSEC المسجلة، وذلك في حال كانت المحللات التي يستخدمها المستخدمين عاجزة عن اتباع الإشارات المقدمة من خلال عملية تغيير مفتاح RFC 5011.

7.2.2 الخلاصة

فمن غير الممكن استخدام عملية القياس هذه لاختبار فيما لو كانت المحللات قادرة على اتباع عملية RFC 5011 لاختيار قيمة مفتاح تسجيل رئيسي KSK جديد لمنطقة الجذر بشكل تلقائي. حيث يتمثل أفضل ما يمكن إنجازه هنا لتحديد كثافة المستخدم الذي يستخدم المحللات لإجراء مصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC، وبالتالي فإنه يستخدم المحللات التي إما ستدعم RFC 5011 أو بحاجة لتدخل يدوي لتحميل مفتاح الدخول الرئيسي KSK الجديد لمنطقة الجذر في المرحلة الزمنية المناسبة.

ويستخدم ما يقارب 24% من المستخدمين المحللات التي تجري مصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC، وبالتالي من المحتمل أن يتأثر بتغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر. حيث سيعيد الفشل في المصادقة رد SERVFAIL، ويستخدم 11% من كافة المستخدمين مجموعة من المحللات حيث يتسبب رد SERVFAIL من المحلل إلى حل الاستفسار من محلل غير مصادق. ويعني هذا بأنه قد يتأثر 13% من كافة المستخدمين من تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر في حال لم يدرك محللهم بـ RFC 5011 ولن يقوم مدير المحلل بتحميل مفتاح الدخول الرئيسي KSK الجديد لمنطقة الجذر في الوقت المناسب.

ومع ذلك، يستخدم العديد من هؤلاء المستخدمين إحدى خدمات محلل مصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC الأكبر والذي من المفهوم إدراكها RFC 5011 (مثل محللات نظام اسم النطاق DNS الخاصة بـ Comcast)، وبالتالي يعتبر هذا الرقم 13% الحد الأعلى لكثافة المستخدمين ممن يتأثرون بهذه الطريقة.

8 الاختبار

يوجد عنصران مرتبطان بالاختبار. العنصر الأول هو نشاط قياس تأثير تغيير مفتاح الدخول الرئيسي KSK حول العمليات العامة للإنترنت بغرض تقييم مستوى التأثير السلبي الذي قد يوقف العملية. أما العنصر الآخر فهو النشاط المتعلق بتحضير الأطراف المعتمدة للعملية، بما فيها مصادر قاعدة الاختبار لإجراء التقييم الذاتي. وقد يجري شركاء القناة التقييم الذاتي بوضع برمجيات و/أو مشغلات تعمل على توزيع مجموعة من الخوادم، أو أي شخص مهتم.

8.1 اختبار التأثير

لم تغطي الاختبارات المرشحة لهذه الأجزاء من هذا التقرير لقياس نجاح المصادقة بعض ردود الفعل على فشل مصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC. وقد يكون استخدام الدليل ببدء بعض الاستفسارات مع الامتدادات الأمنية لنظام اسم النطاق DNSSEC ومن ثم "تجاوز الفشل" إلى نظام اسم النطاق DNS فيما لو كانت هذه الممارسة تزداد أو (تتدهور) بينما يتم تغيير مفتاح الدخول الرئيسي KSK من إحدى الوسائل لتقييم الضرر. وهذا ما يسمى بالضرر الذي إما الذي يمر عليه دون ملاحظته إلا أنه قد يعتبر مقياس ذو قيمة لدى مراقبة تأثير عملية تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر. فمن المرجح ألا يكشف المستخدمين (على الشاشة) هذا الأمر وبالتالي لن يفتحوا تذكرة إلى مكتسب مساعدة مزود الخدمة.

ولا بد من الاختبارات التي تكشف هذا العمل على أساس دوري (شهرياً) من الآن وحتى نهاية عملية تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر (سواء كانت ناجحة أم لا). وستمنحنا الاختبارات منطلق للمقارنة قبل التغيير.

وبالإضافة إلى الاختبار التلقائي، سوف يحتاج التعاقد مع شركاء القناة أثناء تغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر لتقديم معلومات واضحة أو حقيقية أو شبه حقيقية. وهذا بمثابة عامل محفز لتقديم إشعار مسبق للأطراف المتعاقدة، وتفادي الفترات الزمنية الفاصلة عندما يكون عدد العاملين ضئيل، وتفضيل الأوقات عندما تقدم العقود بسهولة.

8.2 وسائل الاختبار الذاتي

وبقدر تمكين الأطراف المعتمدة على الاختبار الذاتي، ينبغي أن يكون هناك برنامج اختبار يحاكي الاختبار التشغيلي بمعدل تغيير متسارع. وإلى جانب تشغيل الخوادم RFC 5011 على وتيرة متسارعة مع مناطق جذر خاطئة مسجلة، لا بد من تقديم مرتكزات الثقة في "هياكل بيانات أخرى" لتقديمها في أسماء المسار ذاته. حيث سيشجع هذا على إنتاج وسائل أفضل، كأدوات تساعد في فحص المفتاح، وسائل لاكتشاف ما يوجد في المدقق (للاستهلاك المحلي أو عن بعد).

وقد يساعد هذا بالتثقيف في الخوارزميات الجديدة وذلك بالسماح بإدراج وإزالة مفاتيح من معلمات مختلفة.

حيث يعد التوقيت مسألة هامة. وكما أن السرعة ضرورية أكثر من الوقت الحقيقي للسماح بإجراء مراقبة معقولة للعملية. إلا أن الوقت الحقيقي مفيد كذلك في الحد من آثار الاختبار.

وفي نهاية المطاف، لا بد من تناول النزاهة في نظام الجذر. وفيما إذا تم استخدام منطقة الجذر بأكملها كبيانات أم لا أو تم النظر في منطقة مزيفة ممثلة.

ثمة أمثلة حالية لقواعد اختبار من هذا القبيل[24]، [25]والتي قد تستخدم كنموذج للاختبار مستقبلاً.

8.3 برمجيات مشرف مفتاح الدخول الرئيسي KSK ومفتاح تسجيل المنطقة ZSK وعملية اختبار تبادلية التعديل

وبما أنه تتطلب عملية تبادل مفتاح الدخول الرئيسي KSK إجراء تعديلات على الجداول والعمليات الحالية وربما برمجيات تدعم عمليات مفتاح الدخول الرئيسي KSK، لا بد من إجراء فحص دقيق لهذه التغييرات قبل بدء التغيير، وإنشاء المفاتيح على سبيل المثال لا الحصر، وإنشاء DNSKEY RRset مسجلة، ومصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC، وتبادل طلب تسجيل المفتاح KSR/رد المفتاح الموقع SKR، وأي آليات احتياطية، وتدريبات مراسم المفتاح.

9 التنفيذ

تكونت عملية تغيير المفتاح المقترح باختصار بداية في يوليو 2013 وتم فحصها وتحسينها حينئذٍ. وينبغي النظر إلى العملية الموصوفة هنا بصفتها مسودة وقد يعمل شركاء إدارة ملفات منطقة الجذر RZM على تحسينها كذلك قبل التنفيذ.

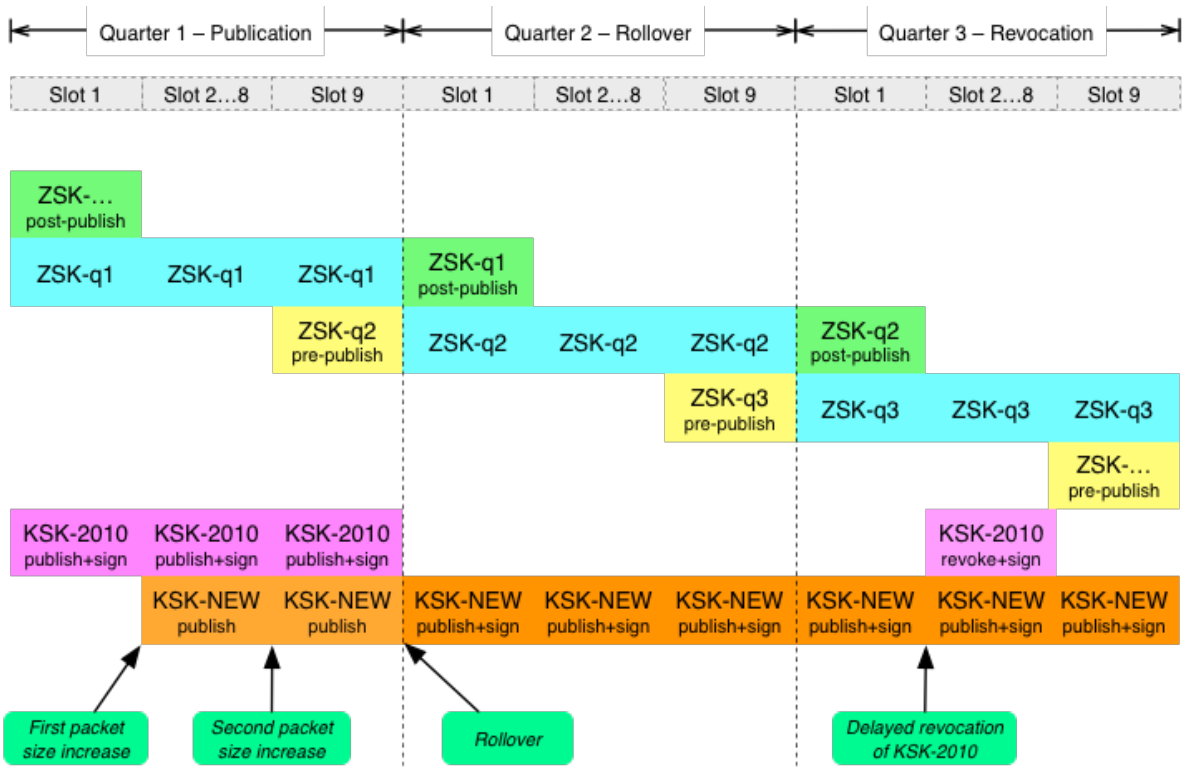
ويتم تقسيم العملية إلى ثلاث مراحل:

1) نشر مفتاح الدخول الرئيسي KSK لمنطقة الجذر المقبلة
2) التغيير إلى التوقيع مع مفتاح الدخول الرئيسي KSK لمنطقة الجذر المقبلة ("التغيير")
3) إلغاء مفتاح الدخول الرئيسي KSK لمنطقة الجذر الحالية.

[24] http://keyroll.systems/
[25] http://icksk.dnssek.info/fauxroot.html

يتم تأخير مفتاح الدخول الرئيسي KSK لمنطقة الجذر الحالي عمداً للسماح بالتراجع، ينبغي أن تبرز أية مشاكل مع مفتاح الدخول الرئيسي KSK لمنطقة الجذر المقبل بعد إزالة مفتاح الدخول الرئيسي KSK لمنطقة الجذر الحالية من مجموعة المفتاح. وتهدف العملية إلى توافقها مع RFC 5011، ومع تمديد النوافذ لإضافة مفتاح الدخول الرئيسي KSK الحالي وإلغاء مفتاح الدخول الرئيسي KSK الحالي. وتتيح هذه العملية بصراحة بالنسبة للخيار بتأجيل الإلغاء لمفتاح الدخول الرئيسي KSK لمنطقة الجذر الحالي لمدة غير محدة، مما يتيح بمراقبة الحالة حيث توجد قضايا غير متوقعة مع عملية التغيير التي تتطلب إجراء تغيير على عملية تغيير المفتاح المخططة.

يظهرالشكل 1 أدناه مراجعة للأرباع الثلاثة أثناء حدوث العملية. لاحظوا أن ترقيم الأرباع مرتبط ببدء العملية، غير مرتبط بتقويم ما. مثلاً، الربع 1 ولا يعني الربع الأول بالضرورة من شهر يناير إلى مارس. ويشار إلى مفتاح الدخول الرئيسي KSK المقبل بـ "KSK-NEW"، أما مفتاح التسجيل الرئيسي KSK الحالي "KSK-2010".



الشكل 1. جدولة التغيير

9.1 نشر مفتاح الدخول الرئيسي KSK المقبل

تتم إضافة مفتاح الدخول الرئيسي KSK المقبل إلى DNSKEY RRset في الفترة الثانية من الربع الأول، إلا أنه لم يتم استخدامه بعد للتسجيل. فهي عبارة عن مرحلة نشر مؤقتة من أجل اختيار مفتاح الدخول الرئيسي KSK المقبل عبر مدققات الامتثال بـ RFC 5011. ويتم نشر مفتاح الدخول الرئيسي KSK المقبل (وتسجيله من خلال مفتاح الدخول الرئيسي KSK الحالي) في منطقة الجذر بما مجموعه 80 يوم قبل استخدامه للتسجيل. ومن المتوقع تحديث مرتكزات الثقة المهيئة يدوياً لإدراج مفتاح الدخول الرئيسي KSK المقبل قبل أو أثناء هذه المدة الزمنية.

ويطلب تغيير الامتثال بـ RFC 5011 بأنه سيتم نشر المفتاح الحديث أثناء مدة لا تتجاوز 30 يوم ("مدة السحب الإضافي"). وفي حال بدت مدة النشر المقترحة من 80 يوم طويلة بشكل غير كافي، فمن المحتمل إدراج ربع أو أرباع نشر إضافية قبل تغيير المفتاح.

وسترى محللات مصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC حجم حزمة الرد على الاستفسار من أجل زيادة DNSKEY RRset لمنطقة الجذر (جحم حزمة الرد) من مجموعة ثمانية 736 إلى 1.022، وذلك خلال ربع نشر مفتاح الدخول الرئيسي KSK المقبل. (تعتمد زيادة هذه الافتراضية على مقارنة حجم رد نظام اسم النطاق DNS في هذه المرحلة في حال لم يكن تغيير المفتاح جارياً على الحجم أثناء عملية تغيير المفتاح.) ويزداد حجم حزمة الرد من مجموعة ثمانية 833 إلى 1,158، وذلك خلال الفترة الأخيرة من الربع الأول.

9.2 التغيير إلى مفتاح الدخول الرئيسي KSK المقبل

وبعد تقديم مفتاح الدخول الرئيسي KSK المقبل، يتم استخدامخ لتسجيل بدء الجذر DNSKEY RRset في الفترة الأولى من الربع الثاني. ويعتبر هذا الربع تماماً كما أي ربع آخر، باستثناء تسجيل كافة DNSKEY RRsets (فقط) مع مفتاح الدخول الرئيسي KSK المقبل. الوقت الذي يتم به نوقيع DNSKEY RRset عبر كل من مفاتيح التسجيل الرئيسية KSKs الحالية والمقبلة أثناء مدة الإلغاء الاختيار، كما هو موصوف أدناه.

9.3 إلغاء مفتاح الدخول الرئيسي KSK الحالي

في حال تم إلغاء مفتاح الدخول الرئيسي KSK الحالي كما هو موصوف في RFC 5011، سيتم نشر مفتاح الدخول الرئيسي KSK الحالي بإزالة البت وتسجيل كل من مفتاح الدخول الرئيسي KSK الحالي والمقبل.

ويعتبر إلغاء مفتاح الدخول الرئيسي KSK الحالي أمر اختياري. وإذا كان الإلغاء مطلوباً، يتم إجراء نشر إلغاء مفتاح الدخول الرئيسي KSK الحالي بدءاً من الفترة الثانية للربع الثالث حتى الفترة الثامنة من الربع الثالث.

ويزداد حجم حزمة الرد أثناء الإلغاء من مجموعة ثمانية 736 إلى 1,297.

9.4 تأثير حجم حزمة الرد

ويتمثل الهدف المرجو في تفادي تجزئ بروتوكول مخطط المستخدم UDP إلى أقصى حد ممكن، وفيما يلي بعض قيود على حجم الرد ذي الصلة:

الحجم	الحدود
مجموعة ثمانية 512	يجب دعم الأدنى من حجم حمولة نظام اسم النطاق DNS من خلال نظام اسم النطاق DNS
مجموعة ثمانية 1,232	حجم حمولة نظام اسم النطاق DNS الأكبر من حزمة بروتوكول مخطط المستخدم UDP لنظام اسم النطاق DNS في الاصدار السادس من بروتوكول الانترنت IPv6 غير المجزأ
مجموعة ثمانية 1,452	حجم حمولة نظام اسم النطاق DNS الأكبر من حزمة بروتوكول مخطط المستخدم UDP لنظام اسم النطاق DNS في الاصدار السادس من بروتوكول الانترنت IPv6 في شبكة الإيثرنت غير المجزأة
مجموعة ثمانية 1,472	حجم حمولة نظام اسم النطاق DNS الأكبر من حزمة بروتوكول مخطط المستخدم UDP لنظام اسم النطاق DNS في الاصدار الرابع من بروتوكول الانترنت IPv4 في شبكة الإيثرنت غير المجزأة

الجدول 4. حدود حجم الحزمة

تشير نتائج الاختبار المقدم سابقاً إلى المشاكل المحتملة مع بعض محللات الاصدار السادس من بروتوكول الانترنت IPv6 وتعاملها مع الردود الكبيرة. وبالتالي يعد حجم القيد الأول والأكثر حضوراً الحد لحزمة بروتوكول مخطط المستخدم UDP لنظام اسم النطاق DNS في الاصدار السادس من بروتوكول الانترنت IPv6 غير المجزأ، الأمر الذي يعني حجم حزمة الرد DNSKEY من مجموعة ثمانية 1,232 على الأكثر.

ويتم التوصل إلى هذا الحد الأول فقط أثناء مرحلة الإلغاء الاختيارية، حيث يجب إعادة تقديم مفتاح الدخول الرئيسي KSK لمنطقة الجذر الحالي والمشار بإلغاء البت. ومن أجل الامتثال الكامل بـ RFC 5011، فإنه من اللازم مضاعفة التوقيع DNSKEY RRset مع كل من مفتاح الدخول الرئيسي KSK لمنطقة الجذر المقبل ومفتاح الدخول الرئيسي KSK لمنطقة الجذر الحالي أثناء مرحلة الإلغاء. وسينجم عن التوقيع المزدوج لـ RRset تجاوز مجموعة ثمانية 1,232 في حجم الرد.

وتكون أكبر حزمة رد مفردة لمنطقة الجذر هي DNSKEY RRset المسجلة. يحتوى الجدول أدناه على مراجعة حجم حزمة رد DNSKEY أثناء التغيير المقترح، بالإضافة إلى المقارنة مع أحجام حزمة الرد غير المبدلة.

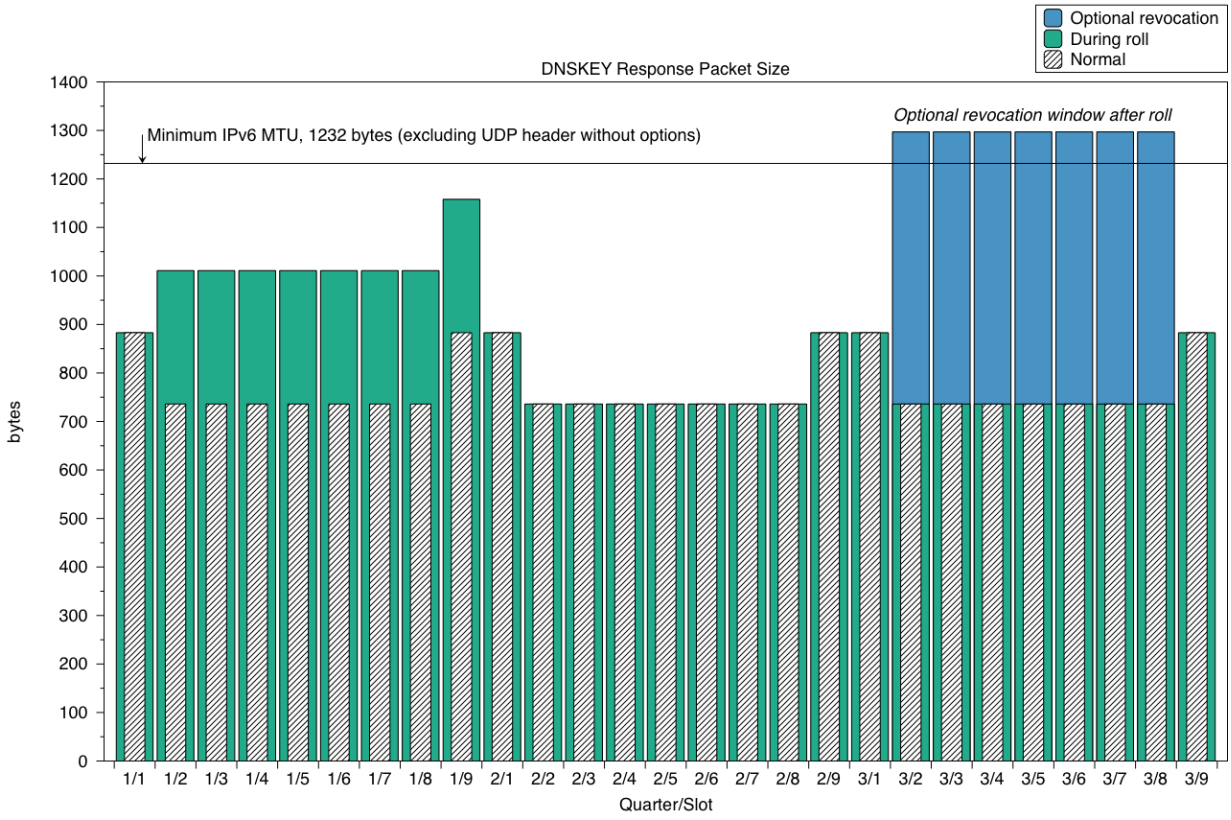
الوقت	DNSKEY أثناء التغيير	RRSIG أثناء التغيير	DNSKEY حجم الرد أثناء التغيير	DNSKEY حجم الرد أثناء عدم التغيير
الفترة الأولى من الربع الأول	1× مفتاح الدخول الرئيسي + KSK 2×مفتاح تسجيل منطقة الدخول ZSK	1× مفتاح الدخول الرئيسي KSK	مجموعة ثمانية 883	مجموعة ثمانية 883
الفترة الثانية من الربع الأول....الفترة الثامنة	2× مفتاح الدخول الرئيسي 1 + KSK ×مفتاح تسجيل منطقة الدخول ZSK	1× مفتاح الدخول الرئيسي KSK	مجموعة ثمانية 1,011	مجموعة ثمانية 736
الفترة التاسعة من الربع الأول	2× مفتاح الدخول الرئيسي 2 + KSK ×مفتاح تسجيل منطقة الدخول ZSK	1× مفتاح الدخول الرئيسي KSK	مجموعة ثمانية 1,158	مجموعة ثمانية 883
الفترة الأولى من الربع الثاني	1× مفتاح الدخول الرئيسي + KSK 2×مفتاح تسجيل منطقة الدخول ZSK	1× مفتاح الدخول الرئيسي KSK	مجموعة ثمانية 883	مجموعة ثمانية 883
الفترة الثانية من الربع الثاني....الفترة الثامنة	1× مفتاح الدخول الرئيسي + KSK 1×مفتاح تسجيل منطقة الدخول ZSK	1× مفتاح الدخول الرئيسي KSK	مجموعة ثمانية 736	مجموعة ثمانية 736

الوقت	DNSKEY أثناء التغيير	RRSIG أثناء التغيير	DNSKEY حجم الرد أثناء التغيير	DNSKEY حجم الرد أثناء عدم التغيير
الفترة التاسعة من الربع الثاني	1× مفتاح الدخول الرئيسي + KSK 2×مفتاح تسجيل منطقة الدخول ZSK	1× مفتاح الدخول الرئيسي KSK	مجموعة ثمانية 883	مجموعة ثمانية 883
الفترة الأولى من الربع الثالث	1× مفتاح الدخول الرئيسي + KSK 2×مفتاح تسجيل منطقة الدخول ZSK	1× مفتاح الدخول الرئيسي KSK	مجموعة ثمانية 883	مجموعة ثمانية 883
الفترة الثالثة من الربع الثاني....الفترة الثامنة	2× مفتاح الدخول الرئيسي 2 + KSK ×مفتاح تسجيل منطقة الدخول ZSK	2× مفتاح الدخول الرئيسي KSK	مجموعة ثمانية 1,297	مجموعة ثمانية 736
الفترة التاسعة من الربع الثالث	1× مفتاح الدخول الرئيسي + KSK 2×مفتاح تسجيل منطقة الدخول ZSK	1× مفتاح الدخول الرئيسي KSK	مجموعة ثمانية 883	مجموعة ثمانية 883

الجدول 5. أحجام الحزمة أثناء التغيير

(يتوافق الترميز اللوني في الجدول أعلاه مع الرسم البياني في الأسفل.)

لم تتم مناقشة المخاطر المرتبطة بتفادي إلغاء المفتاح الصادر بدقة، إلا أنه من الممكن النظر إلى مرحلة الإلغاء على أنها اختيارية في هذه المرحلة. وقد يعنى إحدى الخيارات بتحديث RFC 5011 في هذا الصدد، ودون طلب التوقيع المزدوج لإلغاء مفتاح صادر. وسوف تشتمل المراجعة على المزايا المضافة التي قد ألغاها المفتاح الضائع أو المدمر. ومن الممكن أن يسهل عدم الاضطرار للتوقيع المزدوج مع المفتاح الصادر كذلك في تبادلات المفتاح مستقبلاً، وتغيير الخوارزميات وتغيير طول المفتاح. إلا أنه ونظراً للوقت لإعادة تعريف ونشر ووضع وتوزيع الشيفرة، بالإضافة إلى وضع الشيفرة في العمليات، لا يبدو هذا الخيار مجدياً لتغيير مفتاح الدخول الرئيسي KSK هذا.



الشكل 2. أحجام حزمة الرد DNSKEY

9.5 توزيع خادم الجذر عبر خادم الجذر

حدث عرض الامتدادات الأمنية لنظام اسم النطاق DNSSEC في خادم الجذر عبر خادم الجذر. وظهرت النسخة الأولية من منطقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC الموقعة على خادم واحد في يناير 2010، وخادم جذر آخر في فبراير، وخادمي جذر آخرين في مارس وما شابه ذلك. وكان الهدف بالسماح للخوادم المتكررة (أو ي شيء يرسل استفسارات إلى خوادم الجذر) والقدرة على تجربة الامتدادات الأمنية لنظام اسم النطاق DNSSEC والتراجع في حال لم تكن الأجوبة مقبولة.

حيث تم اقتراح هذه الاستراتيجية لتغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر إلا أنه تم رفضها بسرعة لعدة أسباب. وانطلاقاً من هدف تخفيف المشاكل المرتبطة بمفتاح الدخول الرئيسي KSK لمنطقة الجذر الجديد والقدرة على قياس اعتماد مرتكز الثقة الجديد مع مرور الوقت، فقد اعترضت الحقائق التالية سبيلها.

وبمواجهة فشل مصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC، يتباين التفاعل حسب خادم المصادقة المتكرر من أداة إلى أخرى. وتعرف بعض الأداوت بكونها شديدة العدائية لدى إعادة المحاولة، وبعضها ليس كذلك، وبعضها لا يكترث على الإطلاق.

ويعرف اكتشاف فيما لو قدم خادم متكرر (أو أي مصدر استفسار) قراراً بتفضيل خادم جذر على آخر بأنه أمر غير عملي. ويوجد في الظروف الاعتيادية تتبع غير كافي لمصادر الاستفسار في خوادم الجذر لكشف الخوادم المتكررة التي تفضل خادم جذر على آخر. تعمل مجموعة يومٌ في حياة الإنترنت DITL[26] التي ينفذها مركز عمليات وتحليل وأبحاث

[26] https://www.dns-oarc.net/ditl/2011

نظام اسم النطاق DNS-OARC لمدة قصيرة، وهو بمثابة مشروع ضخم وما زالت لم تتمكن من تغطية كافة خوادم الجذر في أية فترة زمنية.

أما الاعتبار الأخير فهو عبارة عن الفترة الزمنية المتاحة لتقديم مرتكز الثقة الجديد تدريجياً. حيث يوجد 70 يوم فقط في أي ربع خارج مفتاح تسجيل منطقة الجذر ZSK لمنطقة الجذر. ويتطلب إضافة مفتاح الدخول الرئيسي KSK المقبل (إلى الخادم الأول) 40 يوم، مع ترك 30 يوم فقط أو أكثر لإكمال المهمة ضمن إحدى فترات تغيير مفتاح تسجيل منطقة الجذر ZSK. وقد امتد التوزيع المتزايد الأصلي لأكثر من 4 أشهر.

10 الاسترجاع

ينبغي أن يتم التحضير لمجموعة DNSKEY RRset الموقعة فقط من خلال مفتاح الدخول الرئيسي KSK الحالي وتجهيزها للتوزيع وذلك في حالة وجود مشاكل خطيرة كشف عنها بعد تقديم مفتاح الدخول الرئيسي KSK المقبل. وتكون مجموعة RRset هذه بصيغة رد المفتاح الموقّع (SKR) ومن الممكن إصدارها باستخدام مراسيم مفتاح الدخول الرئيسي KSK لمنطقة الجذر ذاتها باعتبارها مجموعة RRset غير مسترجعة. ويستلزم وضع مزيداً من المعايير لهذا الاسترجاع عبر شركاء إدارة ملفات مناطق الجذر RZM.

التوصية 14: وللحد من وقت التعافي نظراً لصعوبة إشراك مفتاح الدخول الرئيسي KSK المقبل، ينبغي إنشاء رد المفتاح الموقّع SKR المنشى فقط عبر مفتاح الدخول الرئيسي KSK الحالي بالتوازي مع رد المفتاح الموقّع SKR المنشئ عبر مفتاح الدخول الرئيسي KSK الحالي.

التوصية 15: ينبغي على شركاء إدارة ملفات منطقة الجذر RZM وضع وتوثيق عملية استخدام رد المفتاح الموقّع SKR المنشى لمفتاح الدخول الرئيسي KSK الحالي.

يتطلب استرجاع رد المفتاح الموقّع SKR والذي يتكون من DNSKEY RRset تحضيرها لكافة أرباع العملية. ويتكون استرجاع رد المفتاح الموقّع SKR أثناء الربع الأول والثاني من مجموعة DNSKEY RRset مع مفتاح الدخول الرئيسي KSK الحالي ومفتاح التسجيل لمنطقة الجذر (مفاتيح) ZSK الحالية، والموقّعة من مفتاح الدخول الرئيسي KSK الحالي. تم حذف مفتاح الدخول الرئيسي KSK المقبل. ويتكون استرجاع رد المفتاح الموقّع SKR أثناء الربع الثالث من مجموعة DNSKEY RRset مع مفتاح الدخول الرئيسي KSK المقبل ومفتاح التسجيل لمنطقة الجذر (مفاتيح) ZSK الحالية، والموقّعة من مفتاح الدخول الرئيسي KSK المقبل. تم حذف مفتاح الدخول الرئيسي KSK الحالي الملغي.

الحدود

تشير الاختبارات لتاريخ توزيع الامتدادات الأمنية لنظام اسم النطاق DNSSEC إلى أنه تحتوي هذه الاختبارات هامش من الخطأ ما يقارب 5%. ويؤخذ هذا ليقصد به أنه يجب على أي بيان مرتبط بكمية الضرر الحاصل إدراك أنه قد يعاني 5% من السكان (الأشخاص أو الخوادم المتكررة اعتماداً على طريقة إجراء التدابير) من تراجع الأداء دون كشف الأمر. ومن هذا المنطلق، لن ينظر إلى تعريف مقياس معين على أنه إحدى الطرق للتوجه نحو تحدد نقطة انطلاق للاسترجاع.

وعلاوة على ذلك، لم يتضح ما شكل الضرر الذي ستتخذه. فقد يكون توزيع مزيف، أو سلسلة مزيفة من التشفير، أو إجراء مزيف أو تصرف عشوائي من الإنترنت. ولهذا السبب، يعد إبقاء العقد مع شركاء القناة وفتح الوسائل لتقديم تقرير عن المشاكل الخطوة الأولى، وباستخدام الحكم حينها للتفاعل مع التقارير.

وإلى جانب شدة الضرر وانتشاره، لم يتضح فيما لو كان يتسبب الإسترجاع ضرراً أكثر من المضي قدماً للتخفيف من المشاكل بينما يتم كشفها، كما هو الحال في وجود العديد من الحالات المستخدمة.

11 متى؟

وبالنظر إلى البيئة التشغيلية الحالية، توجد أربعة أيام في التقويم السنوي عندما يتولى مفتاح الدخول الرئيسي KSK لمنطقة الجذر الجديدة المفتاح الحالي. وتعتبر هذه الأيام الأربعة الأيام الأولى من الأرباع، أو أوائل شهر يناير وأبريل ويوليو وأكتوبر. يحتوي اختيار تاريخ معين لإجراء التغيير على عنصرين - ما هو معقول تشغيلياً وما يتوافق مع النقاشات الحالية فيما يتعلق بانتقال IANA.[27]

ويقصد بمعقول تشغيلياً أنه ينبغي أن تتفادى التواريخ المعينة عطل نهايات الأسبوع، والعطل التي تؤثر على مواعيد العمل، والأوقات عندما يعمل الموظفون على هامش ضئيل. وبالنظر إلى الحاجة لتوافق التواريخ الثلاثة مع الجمهور العالمي، فقد لا يتم استيعاب كل هذا. وبالإضافة إلى التحدي، يبدأ كل ربع يوم الجمعة أو السبت أو الأحد في 2016 و 2017. ولن يبدأ الربع في أي يوم آخر من أيام الأسبوع حتى عام 2018. (يبدأ الربع الرابع في 1 أوكتوبر 2015 يوم الخميس، إلا أنه لن يتم تنفيذ الخطة، ويتطلب إنجاز القليل من الاختبار لإجراء تغيير المفتاح في ذلك التاريخ.)

حيث يعتبر التأثير الغير تقني هي إنتقال دور الإشراف على IANA المخططة. الأمر الذي يجعل من التوصية بتاريخ معين أمر غير عملي في الوقت الراهن.

12 تحليل المخاطر

12.1 المخاطر المرتبطة بالتحضير الغير كافي

الوصف	التأثير	الاحتمالية	التخفيف
لن يكون تغيير مفتاح الدخول الرئيسي KSK مع الخوارزمية ذاتها والتجزية والحجم كافٍ في نظر أصحاب المصلحة	منخفض	غير محتمل	التخطيط لتغيير آخر بمجرد اكمال التغيير الأول؛ وفي حال كانت المعلمات المختلفة مطلوبة، قم بتغييرها
لن يدرك مشغلي الشبكة بالتغيير الحاصل (أي، تحصل مراكز الشبكات NoC على بطاقات المشاكل، وذلك لمعرفة كيفية التصرف)	معتدل	محتمل	في خطة الاتصالات؛ تركيز المشغل

[27] http://www.ntia.doc.gov/press-release/2014/ntia-announces-intent-transition-key-internet-domain-name-functions

الوصف	التأثير	الاحتمالية	التخفيف
لن يحظى مشغلي الشبكة ومطوري البرمجيات (أو "كافة شركاء القناة") على (فرصة الوصول إلى) بيئات اختبار مناسبة	معتدل	محتمل	إعداد قاعدة اختبار RFC 5011 في ICANN مع تغيير متسارع وبموعده؛ إجراء اختبار آخر
لا تكون القدرة على الاختبار أثناء العملية مجدية مركزياً	منخفض	محتمل	وضع أساليب اختبار موزعة؛ وضع قائمة اتصال
انعدام المعايير الحتمية لاتخاذ قرار البدء/عدم البدء	منخفض	محتمل	الحاجة لإعداد الاتصالات والاختبار؛ دراسات جدوى للآليات المستخدمة في المجال؛ جهود طويلة الأمد لوضع مقياس لقبول مرتكز الثقة المحدث

12.2 عدم عمل آلية مرتكز الثقة التلقائية أو غير كافي

الوصف	التأثير	الاحتمالية	التخفيف
عدم تفعيل RFC 5011 في كل مكان	معتدل	محتمل	وسائل إدارة مرتكز ثقة بديلة
تنفيذ RFC 5011 غير مكتمل	معتدل	غير محتمل	التواصل مع مطوري البرمجيات؛ التتأكد من فهم RFC 5011
تنفيذ عملية تمهيد المصادقة غير مكتملة	معتدل	غير محتمل	التواصل مع خبراء تكامل النظام ومعالجي مرتكز الثقة
تحديد عدم توفر مرتكز الثقة من موقع IANA الخاص بـ ICANN	منخفض	غير محتمل	مراقبة التوفر
تحديد المعدات بدون تزامن مرتكز الثقة عبر انعدام الصيانة	منخفض	محتمل	خطة الاتصالات

12.3 تسبب إزالة مفتاح الدخول الرئيسي KSK الحالي بفشل المصادقة

الوصف	التأثير	الاحتمالية	التخفيف
اتباع بروتوكول مرتكز الثقة التلقائي بشكل غير كافي (عبر أي مشترك في العملية)	منخفض	محتمل	الاختبار، الاتصال؛ توفر موارد لمعالجة السرعة للمشغلات
حركة مرتفعة نظراً لإعادة المحاولة في مواجهة الفشل	منخفض	غير محتمل	فحص آثار "التغيير والصياغة[28]"؛ توصيات التخزين السلبي

12.4 تسبب إضافة مفتاح الدخول الرئيسي KSK المقبل تخطي حجم رسالة نظام اسم النطاق DNS الحدود

الوصف	التأثير	الاحتمالية	التخفيف
تسبب إنتقال مجموعات المفتاح إلى زيادة حجم حزم البيانات	معتدل	غير محتمل	تخطيط دقيق للانتقال عبر فحص حجم الرسائل
الإلتباس بشأن التعامل مع تجزئة الاصدار السادس من بروتوكول الانترنت IPv6 في برمجيات نظام اسم النطاق DNS	منخفض	غير محتمل	فحص واختبار برمجيات نظام اسم النطاق DNS

12.5 حدوث أخطاء تشغيلية

الوصف	التأثير	الاحتمالية	التخفيف
سينهي تغيير مفتاح الدخول الرئيسي KSK الفاشل الزخم لاعتماد الامتدادات الأمنية لنظام اسم النطاق DNSSEC	عالي	غير محتمل	تصميم/ مراجعة دقيقة

[28] http://www.potaroo.net/ispcol/2010-02/rollover.html، http://iepg.org/2010-03-ietf77/dnssec-goes-wrong.pdf

الوصف	التأثير	الاحتمالية	التخفيف
يزيد تأجيل تغيير المفتاح حتماً من التأثير في حال أصبح عاجلاً	عالي	غير محتمل	الالتزام بتغيير مفتاح الدخول الرئيسي KSK لمنطقة الجذر
وبمجرد البدء به، لا يمكن العودة إطلاقاً إلى حالة القبول الحالية	عالي	غير محتمل	تحديد خطة بديلة
لم يتم تدمير مفتاح الدخول الرئيسي KSK الحالي (العنصر الخاص) بشكل كافي	منخفض	غير محتمل	الالتزام بإكمال الخطة

13 قائمة فريق التصميم

13.1 متطوعو المجتمع

- جو آبلي .Dyn, Inc كاليفورنيا
- جاب أكيرهويس، NLNetLabs، هولندا
- جون دينكينسون، Sinodun Internet Technologies، المملكة المتحدة
- جيوف هوستون، APNIC، أستراليا
- أوندريج سوري، CZ.NIC، تشيكوسلوفاكيا
- بول ووترز، No Hats/Red Hat، هولندا
- يوشيرو يونيا، JPRS، اليابان

13.2 شركاء إدارة ملفات منطقة الجذر

- ديفيد كونراد، ICANN
- إدوارد لويس، ICANN
- ريتشارد لامب، ICANN
- آليان دوراند، ICANN
- هايلي لافرامبويز، ICANN
- إليز جيريتش، ICANN
- كيم ديفيس، ICANN
- روي آريندز، ICANN
- جاكوب سكيلتر، ICANN
- فريدريك لينجرين، ICANN
- براد فيرد، Verisign
- دوان ويسل، Verisign

- ديفيد بلاكا، Verisign
- آل بوليفار، Verisign
- تيم بولك، US DoC NIST
- سكوت روز، US DoC NIST
- دوغ مونغوميري، US NIST
- آشلي هينيمان، US DoC NTIA
- فيرنيتا هاريس، US DoC NTIA

14 المراجع

- RFC 5011: تحديثات آلية لمرتكزات ثقة الامتدادات الأمنية لنظام اسم النطاق (DNSSEC) https://tools.ietf.org/html/rfc5011
- SAC063: مشورة اللجنة الاستشارية للأمان والاستقرار SSAC المتعلقة بتغيير مفتاح الامتدادات الأمنية لنظام اسم النطاق DNSSEC في منطقة الجذر https://www.icann.org/en/system/files/files/sac-063-en.pdf
- بيان ممارسات الامتدادات الأمنية لنظام اسم النطاق DNSSEC لمشغل مفتاح الدخول الرئيسي KSK لمنطقة الجذر https://www.iana.org/dnssec/icann-dps.txt
- بيان ممارسات الامتدادات الأمنية لنظام اسم النطاق DNSSEC لمشغل مفتاح تسجيل منطقة الجذر ZSK لمنطقة الجذر
- https://www.verisigninc.com/assets/dps-zsk-operator-1527.pdf
- نشر مرتكز ثقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC لمنطقة الجذر https://tools.ietf.org/html/draft-jabley-dnssec-trust-anchor
- إنشاء مرتكز ثقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC مناسب لمنطقة الجذر عند بدء التشغيل https://tools.ietf.org/html/draft-jabley-dnsop-validator-bootstrap

15 الملحق: شركاء القناة

ويشير مصطلح "شركاء القناة" المقبل إلى المنظمات الخارجية التي إما تمكن أو تنقل قيمة إدارة مفتاح الدخول الرئيسي KSK لمنطقة الجذر بشكل مستقل. لا يوجد لدى هذه المنظمات أي علاقات رسمية مع شركاء إدارة ملفات منطقة الجذر RZM، إلا أن التناسق أمر ضروري إلى حد ما. وبالنسبة لكل منظمة، فإنه يتم الاحتفاظ بالاتصالات المناسبة لتبادل الحالة والمعلومات الأخرى المتعلقة بتغير مفتاح الدخول الرئيسي KSK لمنطقة الجذر.

ويتم إدراج شركاء القناة دون ترتيب معين.

15.1 منتجو البرمجيات

يتعلق الاتصال الموضوعي مع هؤلاء الشركاء بتنفيذ إدارة مرتكز ثقة RFC 5011 في البرمجيات (أو لا). وتتكون مجموعة الشركاء من هؤلاء مع مصادقة خوادم تخزين متكررة. لن يتم إدراج معلومات الاتصال مع هؤلاء المنظمات في هذه الوثيقة.

- ISC's BIND (http://www.isc.org)
- NLNetLab's Unbound (https://nlnetlabs.nl)
- Microsoft Windows Server (https://www.microsoft.com/)
- Nominum's Vantio (http://nominum.com/caching-dns/)
- DNSMASQ (http://www.thekelleys.org.uk/dnsmasq/doc.html)
- IRONSIDES (http://ironsides.martincarlisle.com)
- Infoblox (http://www.infoblox.com/
- Secure64 DNS Cache (http://www.secure64.com/)

15.1.1 مُعلق

ناقشت مجموعة الشركاء التالية خوادم مصادقة خوادم تحزين متكررة للامتدادات الأمنية لنظام اسم النطاق DNSSEC إلا أنها لم تصدرها. وهي موجودة على القائمة لإدراجها في حال تم توزيع الشيفرة. (لا تعتمد خوادم تخزين متكررة أخرى لنظام اسم النطاق DNS دون الامتدادات الأمنية لنظام اسم النطاق DNSSEC على مفتاح الدخول الرئيسي KSK لمنطقة الجذر)

- خادم متكرر لـ CZ.NIC's TBD (بعيداً عن Knot)
- PowerDNS TBD

15.2 خبراء تكامل النظام

ينقل شركاء القناة هؤلاء مفتاح الدخول الرئيسي KSK لمنطقة الجذر كجزء من تهيئة المعلومات المعنية، وذكرت برمجيات نظام اسم النطاق DNS في بعض الحالات سابقاً. ومن المتوقع أن تراجع هذه المنظمات مفتاح الدخول الرئيسي KSK لمنطقة الجذر المقبل وإدراجها في تحديثات برمجياتهم.

15.2.1 Linux

- Red Hat Enterprise Linux (RHEL) RPM's
- Micro Focus International's SUSE (RPM's)
- Fedora
- CentOS

- Debian and Canonical (Ubuntu) APT
- Montavista Linux

BSD 15.2.2

- FreeBSD ports
- NetBSD pkgsrc
- OpenBSD ports

15.2.3 أخرى

- Apple iOS، OS X
- Google Android، ChromeOS
- Microsoft
- Cisco
- Juniper
- Belkin
- Cisco / Linksys
- (RTOS) Wind River
- (RTOS) QNX
- OpenVMS
- OpenWRT

15.3 مشغلات المحلل العام

يتم إبلاغ هؤلاء الشركاء بتشغيل خوادم نظام اسم النطاق DNS، لمصادقة الامتدادات الأمنية لنظام اسم النطاق DNSSEC في بعض الحالات. ومن المتوقع أن يدرج هؤلاء الشركاء مفتاح الدخول الرئيسي KSK لمنطقة الجذر باعتبارها تهيئة بيانات، بما أنه قد يكون هناك مراجعات داخلية تتطلب المعرفة بمفتاح الدخول الرئيسي KSK لمنطقة الجذر المقبل.

- Google Public DNS
- OpenDNS
- Neustar DNSAdvantage
- Symantec ConnectSafe
- المستوى 3
- Censurfridns
- Comodo
- Dyn Internet Guide
- Liquid Telecom

وبالإضافة إلى قائمة المشغلات أعلاه من المحللات العامة، والتي تم اختيارها اعتماداً على الحركة المتقبلة من أي مكان في الإنترنت (كما يمكن رؤية الأمر إلى الآن)، قمة شركاء يشغلون المحللات العامة مع قيود على قاعدة الطرف الذي يعتمدون عليه. وكما تم تحديد هؤلاء الشركاء، فإنه سيتم تقديم إشعارات لهم في فعاليات مفتاح الدخول الرئيسي KSK لمنطقة الجذر.