تحليل فني للبنية التحتية الأساسية للمفتاح العام (RPKI)

مكتب المسؤول الفني الأول في ICANN

ألين دوراند

OCTO-014
2 أيلول 2020

ICANN

قائمة المحتويات

هذه الوثيقة جزء من سلسلة مستندات لمكتب المسئول الفني الأول. يُرجى الاطلاع على صفحة إصدارات مكتب المدير الفني المسؤول OCTO للحصول على قائمة بالمستندات الموجودة في السلسلة. إذا كانت لديك أسئلة أو مقترحات حول أي من هذه المستندات، يرجى إرسالها إلى octo@icann.org.

الملخص التنفيذي

إن بروتوكول البوابة الحدودية (BGP) هو بروتوكول التوجيه الذي يستخدمه موفرو خدمة الإنترنت (ISP) عبر الإنترنت. وقد ظل هذا البروتوكول مستخدماً منذ تسعينيات القرن الماضي. تُعرف حوادث توجيه بروتوكول البوابة الحدودية BGP - مثل تسرب مسار YouTube الذي تم الإعلان عنه على نطاق واسع والذي تم من قبل شركة تيليكوم الباكستانية في عام 2008- باسم حالات تسرب المسار والتي يمكن أن تؤدي إلى تحويلات في حركة مرور البيانات عبر الإنترنت. وهي تحدث الآن يومياً وتشكل جزءاً كبيراً من عمليات مزودي خدمة الإنترنت. وقد تأتي هذه التحويلات نتيجة أخطاء في التكوين البرمجي أو بسبب عيوب في البرامج أو في حالات الهجوم الفعالة. والسبب الأساسي لهذه المشكلات هو الافتقار إلى الأمان المضمّن في بروتوكول البوابة الحدودية BGP.

لقد كان ولازال تحديث وتطوير الأمان مهمة طويلة وصعبة وغير مكتملة رغم كل الجهود المبذولة بهذا الصدد. ويطلق على الجهود الأكثر تقدماً المتاحة للنشر والاستخدام اليوم اسم توثيق مصدر البنية التحتية الأساسية للمفتاح العام RPKI. ويستخدم توثيق مصدر البنية التحتية الأساسية للمفتاح العام (مصدر PKI أو RPKI)، وهي عبارة عن إطار عمل هرمي يعمل على تشابك تصديقات المفتاح العام X.509 التي تم إرساؤها في سجلات الإنترنت الإقليمية (RIR) ضمن وشيجة ونسق معينين. ويتمثل هدفها في التحقق من أن مزودي خدمة الإنترنت القائمين بإنشاء مسارات الإنترنت مرخص لهم القيام بذلك من قبل مالك قوائم عناوين بروتوكول الإنترنت (IP) ذات الصلة. وقد كانت عملية توثيق مصدر البنية التحتية الأساسية للمفتاح العام RPKI معمول بها منذ عام 2011 تقريباً. وهي الآن تحظى بالدعم والتأييد في ذروة العديد من العوامل، التي تشمل الجهود التي تقودها سجلات الإنترنت الإقليمية على مدار عدة سنوات لترقيتها وتدريب المهندسين على كيفية استخدامها؛ وجهود المعايير المتفق عليها لأمن التوجيه في جمعية الإنترنت (MANRS)؛ بالإضافة إلى تمويل وزارة الأمن القومي في الحكومة الأمريكية لتطوير برامج البنية التحتية الأساسية للمفتاح العام. وقد أدى ذلك - بالإضافة إلى الاستياء المتنامي تجاه التسربات الحاصلة بانتقال البيانات التي تؤدي إلى الإحساس بأنه "لابد من القيام بشئ"، فضلاً عن النماذج التي أقرّتها بعض كبريات شركات توفير الخدمات (مثل Cloudflare وNTT)- إلى جعل توثيق مصدر البنية التحتية الأساسية للمفتاح العام موضوعاً بالغ الأهمية في عام 2020.

ومع ذلك، فإن التكنولوجيا لا تزال في مرحلة التطوير. كما أن هناك مشكلات خطيرة تفضي إلى تأخير في نشر المعلومات، الأمر الذي يقلل مما لدى مزودي خدمة الإنترنت من مرونة في التعامل مع حالات الطوارئ وإحداث نقاط ضعف في النظام. فنظام البنية التحتية الأساسية للمفتاح العام PKI بحد ذاته قد يتعرض لهجوم. وقد يكون من الصعب اكتشاف حالات الفشل الكارثية وحتى التعافي منها يكون أكثر صعوبة. وتتضاعف تلك المخاطر بنموذج النشر الذي يستخدم خمسة من مراسي الثقة، مما يفسح المجال أمام احتمالية عدم دقة البيانات ويمهد الطريق أمام استخدام عدد أكبر من مراسي الثقة. أما الجهات التي لا تستخدم على الإطلاق البنية التحتية الأساسية للمفتاح العام RPKI فيمكن أن تصبح أيضاً ضحايا غير مباشرة لأي اختراق في أي من مراسي الثقة. ويعتبر السجل الأمريكي لأرقام الإنترنت (ARIN) مخاطر المسئولية والتبعات الناجمة عن تلك السيناريوهات بالغة الأهمية لدرجة أن سجل الإنترنت الإقليمي يطالب بتعويض من أي أطراف معتمدة نظير استخدامها لبيانات البنية التحتية الأساسية للمفتاح العام RPKI. وقد قام النظام بزج سجلات الإنترنت الإقليمية RIR في التشغيل اليومي للإنترنت كمشاركين فاعلين، وهو دور قد يكونوا أو لايكونوا مؤهلين للقيام به، حيث حصلت بعض الحوادث الأخيرة.

والأكثر خطورة من ذلك، فإنه بتقييد نطاق مصدر إعلانات التوجيه، فإن توثيق مصدر البنية التحتية الأساسية للمفتاح العام لا يوفر الحماية إلا من بعض أنواع الهجوم الأكثر بساطة على نظام التوجيه. فأي نظام متين لأمان التوجيه يتطلب تصديقاً كاملاً للمسار، لكن ذلك يعتبر أمراً أكثر تعقيداً.

ويرى عدد من موفري خدمة الإنترنت ونقاط تبادل شبكات الإنترنت (IXP) وموفري السحابة الإلكترونية، أن توقف تسربات البيانات المنتقلة الحاصلة بسبب التكوينات البرمجية الخاطئة والعيوب البرمجية في توثيق مصدر البنية التحتية الأساسية للمفتاح العام دليلاً كافياً على التحسن والتطور التشغيلي وأنه يستحق التكاليف المصروفة على نشر واستخدام هذا النظام المعقد للغاية. ومع ذلك، يجب على من يخطط لنشر واستخدام توثيق مصدر البنية التحتية الأساسية للمفتاح العام أن يكون على دراية بالمشكلات الحالية المتعلقة بالإدراك الكامل لهذه المشاكل إضافة إلى المخاطر التشغيلية المرتبطة بها. وحتى الآن، فإن تأمين البنية التحتية للتوجيه والتي تنطوي ببساطة على نشر واستخدام برنامج ما، ليست بالمسألة السهلة. فلابد من تحقيق التوازن بمنتهى العناية عند محاولة التوفيق بين أمن البروتوكول والتعقيد التشغيلي.

يرجى الاطلاع على إصدار مكتب المسئول الفني الأول رقم 014 للاطلاع على الوثيقة الكاملة (باللغة الإنجليزية).

الخاتمة

هناك اهتمام كبير بالبنية التحتية الأساسية للمفتاح العام RPKI، وهذا الاهتمام موجه من قبل سجلات الإنترنت الإقليمية وشركات مشغلي الشبكات، سواء الكبرى أو الصغيرة. ويرى العديد من الأطراف أن هناك ما يكفي من النتائج المثمرة في بنية RPKI حيث أن عائدات الاستثمار إيجابية. وقد بات توقيع التصديقات على مصدر البيانات بسيطاً بما يكفي لدرجة أن أي مالك لعنوان IP يمكنه القيام بذلك كما أن توثيق مصدر البنية التحتية الأساسية للمفتاح العام يوفر حماية ضد أخطاء الكتابة على لوحة المفاتيح وأخطاء التكوين والعيوب البرمجية. وعلى الرغم من أن توثيق مصدر البنية التحتية الأساسية لا يحمي من الهجوم غير العادي على نظام التوجيه، فمن منظور المشغلين، فإن كلا نوعي الهجوم على نظام التوجيه وحالات تسرب البيانات الحاصلة بسبب أخطاء الكتابة على لوحة المفاتيح تؤدي إلى استصدار شكاوى فنية يجب التعامل معها ومعالجتها. وأي مساعدة سيوفرها توثيق مصدر البنية التحتية الأساسية للمفتاح العام في تلك الجبهة سيكون بالتأكيد محل ترحيب من قبل العديد من مزودي خدمة الإنترنت.

وعلى الرغم من ذلك، فإن النظام برمته - الذي يعتمد على شهادات X.509- هو نظام معقد. ويهئ هذا المستوى من التعقيد إلى إمكانية وجود خطر يتمثل في أن تلك الأخطاء الجديدة والأخطاء الكتابية وأخطاء لوحة المفاتيح سوف تجد طريقها إلى البنية التحتية الأساسية للمفتاح العام نفسها. وستبقى الخبرات العملية التنظيمية القوية في مجال إدارة نظام التشفير على الأرجح مطلباً أساسياً لتنفيذ المصادقة على مصدر البيانات. علماً بأن بنية RPKI بحد ذاتها لا تأتي أبداً بدون مشكلات. فالتأخر في النشر والتوزيع الذي قد يصل إلى 24 ساعة - مقروناً بانعدام المراقبة النظامية واسعة النطاق - قد يمثل مشكلة تشغيلية كبيرة. وتجدر الإشارة أيضاً إلى أنه علاوة على عدم معالجة جميع جوانب مشكلة أمن التوجيه، فإن توثيق مصدر البنية التحتية الأساسية للمفتاح العام يمكن أن يؤدي الى حدوث تهديدات جديدة على نظام التوجيه، كما يحدث في حالة الهجوم على مستودعات بنية RPKI، أو مختلف التصديقات، أو نظم توزيع تصديقات مصدر البيانات (ROA). وحتى يومنا هذا، فقد تم نشر تصديقات مصدر البيانات (ROA) لتوثيق مصدر RPKI على نطاق ضيق. وما تزال هناك أسئلة لم تتم الإجابة عنها فيما يخص مرونة المنظومة ككل للتوسع والتطوير.

وفي نهاية المطاف، سواء كانت تكلفة البنية التحتية الأكثر تفصيلاً والتعقيد التشغيلي لتوثيق مصدر RPKI يستحق قيمة المنفعة من حيث تكامل وصحة التوزيع إلا أنه قرار يجب اتخاذه من قبل مشغلي الشبكات. فبعض مشغلي الشبكات القلقين من التسريبات الحاصلة بسبب سوء التكوين والضبط والتي قد تؤثر على عملياتهم الخاصة بهم يعتقدون بوضوح أن هذا هو ماينبغي عليه أن يكون، في حين أن آخرين ممن يساورهم القلق حيال أمن التوجيه لم يقتنعوا بذلك لغاية الآن. وربما يكون من الضروري الإشارة إلى أن بنية RPKI لا تنطوي على تغييرات نوعية على الهياكل التشغيلية الحيوية للإنترنت ككل. ولا يزال من غير الواضح ما إن كانت المجتمعات المشاركة والمتأثرة بتلك التغييرات على دراية بتلك التأثيرات أم لا. فالمزيد من العمل في مجال التثقيف بخصوص تأثيرات بنية RPKI مبرر بشكل واضح.

شكر وتقدير

على الرغم من أن جميع الآراء الواردة في التقرير هي نفس آراء الكاتب، نود تقديم الشكر والعرفان لمن قدم لنا إسهاماً أو تعقيباً أو أجرى مراجعات خلال فترة وضع هذا التقرير، وهم:

- آلان آيينا، WACREN
- روب أوستين، Hacntr
- جون كوران، ARIN
- كيم ديفيز، ICANN (هيئة الأرقام المخصصة للإنترنت)
- جيوف هيوستن، APNIC
- فريدريك كورسباك، Amazon
- ناتالي كوناكي-ترينامان، RIPE NCC
- مارتن ليفي، Cloudflare
- داي ما، ZDNS
- تيري مانديرسون، ICANN (نظام أسماء النطاقات وهندسة الشبكات)
- كارلوس مارتينيز، LACNIC
- كرستوفر مورو، Google
- ريكاردو باتارا، مركز معلومات الشبكة بالبرازيل
- أمريش فوكير، AFRINIC

- أدريه روباكيفسكي، ISOC
- جوب سنايدرز، NTT
- بيل وودكوك، PCH

والشكر الخاص موصول إلى ديفيد هوبرمان من ICANN، على دعمه المتواصل وقبوله القيام بأعمال التنقيح والمراجعة أثناء كتابة هذا المستند.