资源公钥基础设施 (RPKI) 技术分析

ICANN 首席技术官办公室

阿兰 • 杜朗德 (Alain Durand)
OCTO-014
2020 年 9 月 1 日

ICANN

目录

本文档是首席技术官办公室 (OCTO) 文档系列的一部分。请参阅 OCTO 文档页面，以了解该系列的文档列表。关于这些文档，如果您有任何问题或建议，请将您的反馈发送至 octo@icann.org。

执行摘要

《边界网关协议》(BGP) 是互联网服务提供商 (ISP) 在互联网上使用的路由协议。自 20 世纪 90 年代初以来，它就一直存在。BGP 路由事件（例如，众所周知的 2008 年巴基斯坦电信局导致 YouTube 路由泄漏）也称作“路由泄漏”，可能会造成互联网范围内的流量转移。如今，此类事件每天都在上演，ISP 运营因此而面临巨大损失。这些流量转移可能是配置错误、软件缺陷或主动攻击产生的结果。造成这些问题的根本原因是 BGP 协议缺乏内置的安全性。

改进安全性是一项长期、艰巨且尚未完成的事业。目前，最先进的部署方法是 RPKI 源验证。RPKI 源验证使用资源公钥基础设施（资源 PKI，或简称 RPKI），这是一种分层框架，联锁了锚定在地区互联网注册管理机构 (RIR) 的 X.509 公开密钥证书。其目的在于验证发起互联网路由的 ISP 是否得到相应互联网协议 (IP) 地址块持有者的授权。自 2011 年以来，RPKI 源验证一直存在。正是由于以下多种因素的共同作用，促成这种方法现在越来越受到关注：RIR 多年来主推这种方法并围绕使用方法对工程师开展培训；国际互联网协会努力推动《路由安全相互协议规范》(MANRS)；以及美国国土安全部设立了 RPKI 软件开发基金。此外，随着人们对路由泄漏日渐厌恶，进而意识到“需要采取措施”；再加上一些大型提供商（如 Cloudflare 和 NTT）发挥的榜样作用，使得 RPKI 源验证成为 2020 年的热门话题。

然而，这项技术并非成熟。严重的扩展问题会导致传播延迟，进而降低了 ISP 处理突发事件的灵活性，并且造成相关系统变得脆弱。资源 PKI 系统本身可能会受到攻击。灾难性的故障场景可能难以发现，甚至更难恢复。这些风险还因为使用五个信任锚的部署模型而变得更加复杂，这可能造成数据不一致，并导致信任锚数量增多。完全不使用 RPKI 的当事方也可能会成为任何使用信任锚的一方执行违规操作的间接受害者。美洲互联网号码注册管理机构 (ARIN) 认为这些情况的责任风险非常高，因此 RIR 要求任何依赖方需针对使用其 RPKI 数据而提供赔偿。最近发生的一些事件表明，该系统致使 RIR 陷入一种作为积极参与者投入到互联网日常运营的状态，他们可能最适合也可能不适合发挥这种作用。

更关键的是，由于将保护范围限制在路由公告的源，因此 RPKI 源验证仅能保护路由系统免遭最幼稚的攻击。可靠的路由安全系统要求执行完整的路径验证，但是这个过程要复杂得多。

许多 ISP 、互联网交换点 (IXP) 和云提供商都认为，采用 RPKI 源验证来阻止因错误配置和软件缺陷导致的路由泄漏足以改善运营，部署这个相当复杂的系统是值得的。不过，任何考虑部署 RPKI 源验证的人都应该了解当前存在的成熟度问题以及与之相关的运营风险。保护路由基础设施并不是一个简单的软件部署问题。必须审慎权衡如何取舍协议安全性与操作复杂性。

有关完整文档（英文版），请参阅 OCTO 文档 014。

结论

在大大小小的 RIR 和网络运营商的推动下，RPKI 引起了人们极大的兴趣。许多相关方认为，RPKI 拥有足够多唾手可得的成果，能够带来正向的投资回报。现在，签署路由源声明 (ROA) 的过程已变得相当简单，几乎任何 IP 地址持有者都可以签署，并且 RPKI 源验证提供了抵御“胖手

指失误”、配置错误和软件缺陷的保护措施。尽管 RPKI 源验证不能防御针对路由系统的非幼稚攻击，但是从运营商的角度来看，针对路由系统的幼稚攻击和非幼稚攻击以及由“胖手指失误”引发的路由泄漏都会生成必须处理的工单。毋庸置疑，RPKI 源验证在前端提供的任何帮助都将获得多数 ISP 的欢迎。

但是，基于 X.509 证书的整个系统是比较复杂的。这种复杂性引入了以下风险：新的错误、键入错误和“胖手指失误”将会找到它们在资源 PKI 自身中“兴风作浪”的方式。启用路由源验证 (ROV) 的前提条件可能依然是：在加密系统管理方面，拥有强大的组织专业知识。RPKI 自身并非没有问题。长达 24 小时的传播延迟，加之缺乏普遍的系统性监控，这可能会成为一个主要的运营问题。另外，还值得注意的是，除了无法解决路由安全问题的所有方面之外，RPKI 源验证还可能会给路由系统造成新的威胁，例如，可能会攻击资源 PKI 存储库、各种证书或 ROA 分发系统。迄今为止，RPKI 源验证 ROV 仅部署在有限的范围内。在整个系统的缩放性方面，仍然存在着一些尚未解决的相关问题。

最终，网络运营商需要决定：与在路由完整性方面获得的利益相比，RPKI 源验证投入的相当详细的基础设施和运营复杂性成本，是否物有所值。有些网络运营商曾担心因配置错误引发的路由泄漏会对其运营产生影响，所以清楚地认识到这种情况；然而其他关心路由安全的网络运营商尚未确信这种情况。或许更为重要的是，RPKI 确实意味着要对整个互联网的关键运营结构执行某些更改。尚不清楚参与这些更改以及受其影响的社群是否充分意识到这些影响。显然有必要进一步围绕 RPKI 的含义开展交流。

致谢

尽管本报告中的所有观点均出自于作者本人，但我们仍要感谢以下人员在本报告编写过程中提供的意见、反馈或评论：

- 来自西非和中非教育研究网络 (WACREN) 的阿兰·艾伊纳 (Alain Aina)
- 来自 Hacntr 的罗伯·奥斯汀 (Rob Austein)
- 来自美洲互联网号码注册管理机构 (ARIN) 的约翰·柯伦 (John Curran)
- 来自 ICANN 互联网号码分配机构 (IANA) 的金·戴维斯 (Kim Davies)
- 来自亚太互联网络信息中心 (APNIC) 的吉奥夫·休斯顿 (Geoff Huston)
- 来自 Amazon 的弗雷德里克·科斯巴克 (Fredrik Korsback)
- 来自欧洲网络协调中心 (RIPE NCC) 的娜塔莉·肯纳克-特雷纳曼 (Nathalie K ünnake-Trenaman)
- 来自 Cloudflare 的马丁·勒维 (Martin Levy)
- 来自互联网域名系统北京市工程研究中心有限公司 (ZDNS) 的马迪 (Di Ma)
- 来自 ICANN（域名系统 (DNS) 及网络工程部）的特里·曼德尔森 (Terry Manderson)
- 来自拉丁美洲和加勒比海地区互联网地址注册管理机构 (LACNIC) 的卡洛斯·马丁内斯 (Carlos Martinez)
- 来自 Google 的克里斯托弗·莫罗 (Christopher Morrow)
- 来自巴西网络信息中心 (NIC) 的里卡多·帕塔拉 (Ricardo Patara)
- 来自非洲网络信息中心 (AFRINIC) 的阿姆雷什·普科克 (Amreesh Phokeer)
- 来自国际互联网协会 (ISOC) 的安德烈·罗巴切夫斯基 (Andrei Robachevsky)
- 来自 NTT 的乔布·斯尼德斯 (Job Snijders)

- 来自 PCH 的比尔·伍德科克 (Bill Woodcock)

特别感谢 ICANN 的戴维 • 胡博曼 (David Huberman)，感谢他在我撰写本文档期间给予的持续不断的支持以及愿意担当决策咨询人。