Resource Public Key Infrastructure (RPKI) Technical Analysis

资源公钥基础设施（(RPKI)技术分析

ICANN 首席技术官办公室(ICANN Office of the Chief Technology Officer)

阿兰·杜朗德(Alican Durand)

OCTO-014
2020 年 9 月 2 日

中文翻译：秦超逸，刘天资，张宇
哈尔滨工业大学网络空间安全学院

2020 年 9 月 24 日(初版)，12 月 9 日(修改)

目录

0 执行摘要

边界网关协议(Border Gateway Protocol，BGP)是互联网服务提供商(Internet Service Providers，ISP)在互联网上使用的路由协议。该协议自 90 年代初以来一直使用。BGP 路由事故，例如被广泛宣传的 2008 年巴基斯坦电信造成的将 YouTube 路由泄露，被称为路由泄露，并能够造成互联网范围内的流量转移。现在这些事故每天都在发生，并且导致 ISP 业务为此付出巨大代价。这些流量转移可能是配置错误、软件错误或者主动攻击的结果。这些问题的根源在于 BGP 协议缺乏内建的安全性。

改进安全性是一项长期、困难且未竟的努力。今天可用于部署的最先进的工作称为 RPKI 起源验证。RPKI 起源验证使用资源公钥基础设施(Resource Public Key Infrastructure, Resource PKI，或 RPKI)，这是一个将 X.509 公钥证书连锁的层次化框架，这些证书以多个 RIR(Regional Internet Registries，区域互联网注册机构)为锚点。它的目标是为了验证声明起源互联网路由的 ISP 是由相应的 IP (Internet Protocol，互联网协议)地址块的持有者所授权而实施的。RPKI 起源验证工作从 2011 年左右持续到现在。它现在在多个因素的累积作用下开始流行，包括 RIR 多年来所领导的推广和培训工程师如何使用它的努力；互联网协会(Internet Society)在路由安全互相同意规范(Mutually Agreed Norms for Routing Security，MANRS)的努力；以及美国国土安全部对 RPKI 软件开发的资助。此外，加上对路由泄漏越来越难以忍受，导致人们感觉到“需要做些什么了”，再加上一些大型提供商(如 Cloudflare 和 NTT)的示范，使得 RPKI 起源验证在 2020 年成为一个热门话题。

然而，这项技术还不成熟。存在严重的可扩展性问题，这导致传播延迟，进而降低了 ISP 处理紧急事件的灵活性，给整个系统带来了脆弱性。RPKI 系统本身可以被攻击。灾难性的故障场景可能很难被检测，甚至更难恢复。使用五个信任锚的部署模型使这些风险更加复杂，这可能造成数据不一致，甚至导致信任锚数量增多。完全不使用 RPKI 的参与者也可能成为任何一个信任锚的违规的附带受害者。美洲互联网号码注册管理机构(American Registry for Internet Numbers，ARIN)认为这些情况下的责任风险非常高，以至于该 RIR 要求任何依赖方对 RPKI 数据的使用进行免责。RPKI 系统已将 RIR 作为积极参与者投入到互联网的日常运营中，正如一些最近的事故所表明，它们可能最适合也可能不适合担任这一角色。

更关键的是，通过将保护范围限定为路由声明的起源，RPKI 起源验证仅保护路由系统免受最初级的攻击。一个健壮的路由安全系统需要完整的路径验证，但那要复杂得多。

许多 ISP、互联网交换点(Internet exchange point, IXP)和云提供商认为，通过 RPKI 起源验证来阻止来自错误配置和软件错误的路由泄漏足以作为一项运营改进，部署这个相当复杂的系统的成本是值得的。不过，任何考虑部署 RPKI 起源验证的人都应该了解当前的成熟度问题和与

之相关的运营风险。保护路由基础设施(截止目前)不是部署一个软件那么的简单问题。在协议安全性和运营复杂性之间必须仔细地权衡。

1 简介

ICANN 的使命是确保互联网唯一标识符系统的稳定和安全运行，并承诺“…维护和加强 DNS 的管理以及 DNS 和互联网的运营稳定性、可靠性、安全性、全局互操作性、弹性和开放性；”[1]。毫无疑问，路由和 IP 地址是 DNS 全球稳定运行的重要因素。为此，ICANN 组织深入研究了 RKPI 及其运行环境和实践，以了解其部署的当前状态，更重要的是，确定潜在风险、挑战和改进机会的领域。我们希望这份文件将有助于在适当的论坛上展开讨论，以便找到本文件强调的一些问题的解决方案。

2008 年被广泛宣传的巴基斯坦电信(Pakistan Telecom)造成的 YouTube 路由泄露事件[2]提供了一个开创性的时刻，使人们更加普遍地认识到边界网关协议(Border Gateway Protocol，BGP)[3]的安全问题。BGP 帮助互联网服务提供商(Internet Service Providers，ISP)进行互连和交换路由，以保持互联网的连通性。在 2008 年的事件中，巴基斯坦电信试图屏蔽被巴基斯坦政府视为令人反感的内容。为了屏蔽这些内容，巴基斯坦电信向 BGP 注入了一条“本地”路由，该路由将 YouTube 地址块路由到不存在的空地址(即“空路由”，null route)。这种“本地” 路由本应只影响本地客户，阻止他们访问 YouTube。但“空路由”泄露给了至少一家为巴基斯坦电信提供国际连接服务的 ISP，并从这些 ISP 向外传播，影响了互联网的大部分区域，并阻止了世界各地互联网上的许多人访问 YouTube。在 2008 年晚些时候，Defcon-16 会议上的一个现场演示[4]展示了实施 BGP 劫持是多么容易。

互联网路由的工作方式如下：一个 ISP(ISP1)将一个客户(客户 1)连接到其网络。ISP1 随后通过 BGP 向所有对等方“通告”客户 1 公共 IP 地址的可达性，以表明 ISP1 与客户 1 有直接连接。然后，这些与 ISP1 对等的 ISP 向他们自己的对等方进行重新通告：他们可以经过 ISP1 与客户 1 有一个一跳的连接。这样，一个称为自治系统路径(Autonomous System Path，AS path)的 ISP 链通过 BGP 协议在互联网上传播。

巴基斯坦电信事件之所以能够发生，根本原因是 BGP 没有内置的授权检查。尽管有早期工作实现基于公开可用的路由数据库对路由通告进行过滤，许多 ISP 还是真诚地接受路由对等方提供的所有路由。其结果是，无论是恶意还是意外造成泄露的路由，都会迅速传播到互联网的各个角落。

1 https://www.icann.org/resources/pages/governance/bylaws-en
2 https://www.nytimes.com/2008/02/26/technology/26tube.html
3 https://tools.ietf.org/html/rfc4271
4 https://www.slideshare.net/nguyenduchaisp21/defcon-16pilosovkapela

BGP 是支撑互联网上所有路由的核心协议，它的起源可以追溯到 20 世纪 80 年代末和 90 年代初。在当时，BGP 的安全问题并没有得到今天这样的重视。路由系统的互操作性、可扩展性、灵活性和稳定性是最重要的考虑因素。RFC 1163[5]定义了 1990 年 6 月发布的 BGP 的原始版本。其中的安全考虑章节说明："安全问题不在本备忘录中讨论。"当时这并不是 BGP 规范所独有的，因为这个时代互联网工程任务组(IETF)发布的许多文件都有类似的文本。

巴基斯坦电信/YouTube 事件绝非罕见。这类事件被称为"路由劫持"或 "路由泄漏"。RFC 7908[6]中提供了完整的路由泄漏分类法。互联网协会(Internet Society，ISOC)支持的共同商定的路由安全规范(Mutually Agreed Norms for Routing Security，MANRS)观测站[7]仅在 2020 年 1 月就报告了 328 条路由泄漏；MANRS 还描述了路由泄露是如何计数的[8]。已报道的许多备受关注的路由泄露事件中，最著名的案例是发生在大约 2017 年的中国电信事件[9]，以及最近于 2020 年 4 月 1 日发生在 Rostelecom 的事件[10]。无论是故意还是意外，此类路由泄漏都会严重破坏互联网流量。

早在巴基斯坦电信/YouTube 事件发生之前，IETF 就很清楚 BGP 的漏洞。在众多工作中，2000 年发表了一篇论文，其章节 4.4 中定义了一种确保协议正确性的框架 Secure BGP(S-BGP)。2006 年，继路由协议安全需求(Routing Protocol Security Requirements，RPSEC)工作组的 RFC 4272[11]之后，IETF 成立了一个工作组来解决路由系统安全问题：这个工作组是安全域间路由工作组(Secure Inter-Domain Routing Working Group，SIDR)[12]，随后成为 SIDR 运营工作组(SIDR Operations Working Group，SIDROPS)[13]。

人们提出了一系列保护 BGP 的技术[14]。IETF 发布了一个"BGP 运营和安全"的最佳当前实践 RFC 7454[15]。在文档中，一方面，我们发现了诸如 TCP 消息摘要算法(Message Digest 5，MD5)选项等技术来确保 BGP 消息不被篡改。另一方面，我们发现了一些试图检查 BGP 通告真实性的技术，如本文章节 4.4 所述。RPKI 起源验证属于后者，也是本文的重点。RFC 7115[16]中记录了 RPKI 起源验证体系结构。

RPKI，或称资源 PKI，是一种通用的公钥基础设施，用于对互联网号码资源(Internet number resources，INR)生成密码学可验证的断言，INR 包括 IP 地址块和自治域(Autonomous System，

5 https://tools.ietf.org/html/rfc1163
6 https://tools.ietf.org/html/rfc7908
7 https://observatory.manrs.org
8 https://observatory.manrs.org/#/about
9 https://dyn.com/blog/china-telecoms-internet-traffic-misdirection/和 https://arstechnica.com/information-technology/2019/06/bgp-mishap-sends-european-mobile-traffic- through-china-telecom-for-2-hours/
10 https://www.securityweek.com/russian-telco-hijacked-internet-traffic-major-networks-accident-or-malicious-action
11 https://tools.ietf.org/html/rfc4272
12 https://datatracker.ietf.org/wg/sidr/charter/
13 https://datatracker.ietf.org/wg/sidrops/charter/
14 http://www.potaroo.net/papers/BGP_Security_Literature_Review.pdf
15 https://tools.ietf.org/html/rfc7454
16 https://tools.ietf.org/html/rfc7115

AS)号。4.4 节描述的一些技术将用于管理所有断言，这些断言将用于实现对 BGP AS 路径的验证。这些技术都没有在运营社区中产生任何显著的吸引力。然而，这个范围更为有限、只集中在路由起源验证上的工作却做到了。该工作也被称为 RPKI，RPKI 这个词混合了两种意思，第一个意思是资源 PKI(Resource PKI)，第二个意思是执行路由起源验证的资源 PKI 的用例。因此，有时后者被称为路由起源验证，但是当我们使用术语路由起源授权(Route Origin Authorization，ROA)和路由起源验证(Route Origin Validation，ROV)时，也会造成混淆。

本文档中使用的术语“RPKI”与 PKI 及其用例是同一个意思。这似乎是在许多关于这个主题的演讲和文章中做出的选择。当 RPKI 这个词的两个意思之间的区别变得重要时，作者将使用术语 RPKI 来讨论分布式公钥/私钥证书数据库，并用 RPKI 起源验证来讨论用例。

RPKI 起源验证于 2011 年首次以当前形式进行了规定。九年来，资助了 RPKI 软件开发[17]的美国国土安全部，加上 ISOC MANRS 运营商组和区域互联网注册机构(Regional Internet Registry，RIR)研讨会的最新工作，引领了该行业构建 RPKI 基础设施的工作。直到两年前，RPKI 起源验证的整体采用率还相当平淡。然而，近年来情况发生了变化，RPKI 起源验证目前是网络运营圈中的一个热点话题。RPKI 起源验证部署是 2020 年 2 月上一届北美网络运营组(North America Network Operation Group，NANOG)的主题之一[18]。其支持者认为，RPKI 是互联网安全、稳定和弹性的重要组成部分。

本文探讨了 PRKI 的技术、运营和法律问题。它会回答以下问题：

- 什么是 RPKI 以及它是如何工作的？
- RPKI 提供什么保护？
- 为什么 RPKI 现在受到关注？
- RPKI 是否可能是实现 BGP 安全的最后一个重要步骤？
- ICANN 和 RIR 在 RPKI 部署中的作用是什么？
- RPKI 对 IP 地址市场有何影响？
- RPKI 的责任考虑是什么？对谁？
- 什么可能是灾难性的 RPKI 故障情况？
- 技术如何演进？

1.1 术语

在本文中定义一些常用术语。

17 https://www.pcworld.com/article/157909/feds_.net_security.html
18 https://www.nanog.org/meetings/nanog-78/agenda/

*IP 地址*是一个数字值，用于在 Internet 协议(IP)中标识网络的终端。在当今的互联网上有两种协议族：IPv4 和 IPv6，IPv4 的数值是从以 32 位表示的数字池中提取的，IPv6 数值是从 128 位的数字池中提取的。

*地址前缀*是一个连续的 IP 地址序列，当用二进制表示法表示时，这个序列共享一个公共前缀。这个以位为单位的公共前缀的长度称为地址前缀的大小。

自治域(Autonomous System，AS)是具有单一管理控制范围的网络，例如 ISP 或大型企业网络。*自治域号*(Autonomous System Number，ASN 或 AS-Number)是一个唯一的号码，通常由一个 RIR 指派(assign)给一个自治域。在 BGP 中这个号码用于标识路由域，通常是 ISP。

*数字资源*是指 IP 地址和 ASN。

*X.509 公钥证书*是证书颁发者所生成的数字证明，用于证明给定的公钥属于证书的主体。

*资源证书*是 X.509 公钥证书的变体，其中证书的颁发者证明公钥的所有者也是一组已列出的数字资源的所有者。资源证书系统被称为资源公钥基础设施(RPKI 或 Resource PKI).

信任锚位置(trust anchor location，TAL)用于描述 RPKI 信任锚可被检索到的位置。TAL 既包含指向信任锚自签名根证书的统一资源标识符(uniform resource identifier，URI)，也包含用于对该资料库进行签名的 base64 编码的公钥[19]。TAL 用作遍历 CA 资料库的 RPKI 树的起点。根证书有一个指向 CA 资料库的特殊属性。每个信任锚或根证书在逻辑上等同于 DNSSEC 的密钥签名密钥(key signing key，KSK)。

*路由泄漏*是“路由通告的传播范围超出其预期范围”(RFC 7908[20])。造成路由泄露的原因包括路由误起源、路由劫持、违反路由策略等。

2 RPKI 背景

IP 地址分配和 IP 网络路由是两个相关但是不同的主题。

IP 地址从 ICANN 分配给区域互联网注册中心(RIR)，作为 ICANN 附属 PTI 执行的 IANA 数字分配服务的组成部分，如 ICANN 和五个 RIR 之间的“IANA 数字分配服务的服务水平协议”所述。RIR 将其分配(allocate)或指派(assign)给网络运营商，如 ISP。当前有五个 RIR，每个“大

19 https://tools.ietf.org/html/rfc8630
20 https://tools.ietf.org/html/rfc7908

洲”服务区域中有一个：非洲的非洲网络信息中心(African Network Information Center，AFRINIC)[21]，亚洲和大洋洲的亚太网络信息中心(Asia Pacific Network Information Center，APNIC)[22]，北美和加勒比部分地区的美洲互联网号码注册处(American Registry for Internet Numbers，ARIN)[23]，拉丁美洲和加勒比地区的互联网地址注册处(Latin American and Caribbean Internet Addresses Registry，LACNIC)[24]，以及欧洲、中东和中亚部分地区的欧洲 IP 网络资源协调中心(Réseaux IP Européens Network Coordination Centre，RIPE-NCC)[25]。(在欧洲服务区域，RIPE 指的是社区，而 RIPE 网络协调中心(RIPE NCC)则指代提供服务的 RIR。这与 ICANN(社区)和 ICANN 组织(支持社区的组织)的区别相似。其他地区不做这种区分。)围绕 IP 地址分配的政策可能因每个地区的互联网社区的利益而有所不同，这些政策是在这些社区内制定的，并由对应区域的 RIR 实施。

当一项政策根据其政策制定过程得到所有五个 RIR 的同意，并需要采取具体行动或结果才能实施时，该政策可以受到全球政策制定过程管理。ICANN 地址支持组织(Address Supporting Organization，ASO)[26]地址理事会(Address Council)[27]，也被称为数字资源组织(Number Resource Organization，NRO)[28]数字理事会(Number Council)[29]，协调全球政策制定过程(Global Policy Development Process)。

从某个 RIR 或 IP 地址市场(目前 RIR 的 IPv4 地址免费池已用尽)获取了 IP 地址块并不保证这些地址可以通过互联网访问。要获得地址块的路由服务，需要将该地址块转换为路由前缀，并让一个或多个 ISP 向互联网的其余部分声明该前缀。ISP 遵循自己的政策，即独立的规则，接受或拒绝来自其对等方和/或客户的此类声明。虽然 ISP 确实在世界各地的网络运营商组织(Network Operator Groups，NOG)中共享经验(并且松散地协作)，但是没有强制性的全局路由策略来设置什么行为是可接受或什么不是。由互联网协会支持的 MANRS[30]工作就是朝着这个方向迈出的一步。

当两个 ISP 互连时，它们通过 BGP 会话交换路由。由于 BGP 协议的性质，网络之间没有一致同意的单一“路线图”–每个路由器都有自己的互联网互连描述，该描述受网络互连拓扑、自己的策略和对等方的策略的影响。具体地，BGP 是一种路径向量协议，是距离向量协议的变体。

21 https://afrinic.net
22 https://www.apnic.net
23 https://www.arin.net
24 https://www.lacnic.net
25 https://www.ripe.net
26 https://aso.icann.org
27 https://aso.icann.org/advisory-council/
28 https://www.nro.net
29 https://www.nro.net/about/address-supporting-organization/
30 https://www.manrs.org/about/

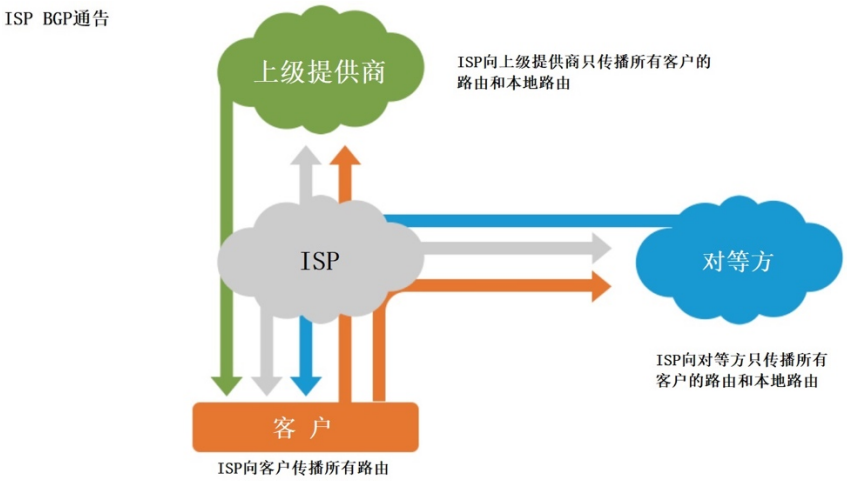
20 世纪 90 年代初，IETF IPIDRP 曾讨论过从 BGP4 迁移到另一种称为 IDRP 的域间路由协议，IDRP 是开放系统互连协议套件的一部分，是一种链路状态协议，除了其他功能之外，它还将提供一个一致同意的互联网完整地图[31]。这项工作没有成功，人们对 IDRP 的兴趣减弱，仍在继续 BGP4 开发。

一个 ISP 只有自己网络的和对等方告诉它的网络的视图。ISP 之间路由的工作方式如下：ISP1 告诉 ISP2 它可以到达哪些前缀，反之 ISP2 也会告诉 ISP1。ISP 与末端客户连接时也有类似的过程。一个问题立刻出现： ISP 应该设置什么过滤器来接受或拒绝来自对等或客户关系的 ISP 的路由声明？

在 ISP 与客户对等(即客户可以是另一个 ISP 或一个叶子网络)的情况下，这个问题的答案通常很简单。客户的地址空间来自 ISP 本身，或者来自不同的 ISP，或者直接从 RIR 获得，并且地址空间的前缀已经被传递给 ISP，可能是在服务合同协商阶段。该 ISP 可以设置一个过滤器，上面写着：我允许我的客户通告注册到他们的地址的路由前缀，但其他的前缀不行。在典型的提供商/客户关系中，提供商需要向其客户通告一个默认路由(当没有其他路由可用时可以使用的路由)和可达路由的完整枚举，其中默认路由指向一个能提供更多信息的路由器。

在 ISP 与 ISP 对等互联(peering)的情况下，过滤什么变得更加复杂。一个 ISP 声明路由的预期行为如下：

- 该 ISP 将向其客户通告从所有其他客户、所有提供商和所有对等方获得的所有路由。
- 该 ISP 将向其上游提供商通告所有客户学习的路由，但不包括对等方学习的路由、提供商学习的路由和所有 ISP 本地的路由。
- 该 ISP 将向对等方通告所有客户学习的路由和所有的 ISP 本地路由，但不包括对等学习的路由和提供商学习的路由。



31 https://ftp.unpad.ac.id/ietf/ietf/ipidrp/ipidrp-minutes-92nov.txt

问题是，ISP2 应该从 ISP1 接受什么？理想情况下，ISP1 将有一个 ISP2 客户前缀的列表，并且只接受这些前缀的通知。然而，这种客户关系通常被视为隐私信息，并不总是公开的。当出现一连串 ISP 时，情况变得更加复杂。ISP 离最初声明前缀的客户越远，评估路由声明的有效性就越复杂。互联网路由注册库(Internet Routing Registry，IRR)和路由策略说明语言(Routing Policy Specification Language，RPSL)RFC 2622[32]用来帮助解决这个问题。

2.1 路由注册：从 IRR 到 RPKI

从概念上讲，互联网路由注册库(Internet Routing Registry，IRR)系统由一组包含路由信息的独立注册库组成，这些独立的注册库具有不同的策略和重叠的数据。IRR 是由许多组织独立开发的工具之一，用于在 ISP 之间共享这些组织有关所声明 IP 地址块的意图的信息。IRR 包含“路由对象”，即 ISP 用于配置路由器和对等互联关系的信息。IRR 还包含其他对象。其中一个对象是“Aut-num”，它被认为是记录网络路由策略的起点，这也是 RPSL 的主要目标。IRR 的起源可以追溯到 20 世纪 90 年代中期，1994 年美国国家科学基金会(National Science Foundation，NSF)对 Merit 网络[33]资助中的一部分用来资助设立一个“路由仲裁者”（routing arbiter）[34]。新兴互联网拥有独立的私人和公共自主的服务平台，以及复杂性不断增加的互联点所适用的政策，而路由仲裁者旨在解决新兴互联网中日益复杂的问题。

全球 IRR 实际上是由 20 多个独立的数据库组成的，这些数据库有时是不一致的。其中一些数据库是公开的，比如 RIPE IRR[35]和路由仲裁器数据库(Routing Arbiter Database，RADb)[36]，有些则不是。ISP 在其中一个或多个数据库中发布其路由策略和声明，然后使用 IRR 构建路由声明过滤器。前提是终端客户的 ISP 在 IRR 中注册了他们的前缀。过滤器将允许他们的 ISP 过滤掉来自客户的任何错误前缀。

一个 IRR 系统面临的主要问题是，在许多情况下，路由注册机构使用“开放写访问”策略：对进入一些数据库的内容几乎没有验证，而对这些 IRR 数据库进行融合时，融合后的数据库也继承了这些真实性存疑的条目。这些数据库中的对象是否是真实的，或者是否后来被篡改，都是未知的。另一个问题是，由于缺乏维护，数据库中的对象往往会很快过时。这些问题使得 IRR 数据的质量受到质疑，将 IRR 数据用于自动构建路由过滤器是有问题的。

RPKI 起源验证可以理解为是在某些方面超越当前 IRR、在其他方面实际不如 IRR 的一项工作。它依赖于一个新的公开分布式数据库，即 RPKI，该数据库将确保哪一方可以对 IP 地址块进行权威发言。一种数字签名的证明，它为具有一个指定 AS 号码的网络提供起源一个 IP 地

32 https://tools.ietf.org/html/rfc2622
33 https://www.nsf.gov/awardsearch/showAward?AWD_ID=9321060
34 https://www.merit.edu/research/projects/
35 https://www.ripe.net/manage-ips-and-asns/db/support/managing-route-objects-in-the-irr
36 https://www.radb.net

址块的权限，这种权限结合了身份验证和不可否认性。然而，RPKI 不能保证数据是最新的：没有任何东西能强迫 IP 地址所有者维护他们的信息，而且 RPKI 中的所有证书都有有效期，在某个时刻证书会超时。证书超时意味着证书的数字签名不能再被验证，证书本身应该被忽略。

根 CA 的有效期通常超过 10 年。ISP CA 有效期通常为一年，具体取决于 ISP CA 与 RIR 的合同。RPKI 也不能保证关联的路由操作会实际发生。前缀所有者在做出这些断言时不需要起源自治系统的许可，并且 AS 所有者没有义务发布特定的声明(参见章节 2.5.1 中的示例)。最后，RPKI 起源验证的范围仅限于前缀的起源点，并且不会说明在网络中传播路由对象所采用的实际路由路径。

与 DNSSEC 一样[37]，RPKI 起源验证有两个操作组件：路由起源声明和签名，与路由起源验证。

生成 RPKI 起源验证对象需要 IP 地址块所有者进行一个可验证的授权，授权内容是一个 AS 可以作为对应前缀的路由通告的起源 AS，授权以附加到 IP 地址所有者权威的数字签名的形式表示。签名使 AS 有权将 IP 地址块所有者的前缀声明到路由系统中，任何其他人，例如对等方或提供商，都可以验证该前缀。

验证路由对象的起源是网络运营商使用的一个过程。通过维护已发布在分布式 RPKI 框架中的所有当前证明的本地副本，网络运营商可以验证所有此类起源声明的真实性。包含所有证明的集合(路由对象和相关的起源 AS)可以用来构造一个过滤器集，并且这个过滤器可以用在 BGP 发言(speaking)路由器上，实现自动接受或拒绝 BGP 路由声明，或者对接收到的 BGP 路由声明进行优先级排序，并确定这些操作是基于真实数据执行的。

2.2 RPKI 起源验证签名：路由起源授权

资源公钥基础设施(Resource Public Key Infrastructure，RPKI)是一个将 X.509 公钥证书连锁的层次化框架。RPKI 目前有五个信任锚，每一个都由一个 RIR 运营。每个信任锚中的资源集覆盖整个互联网数字空间(包括 IPv4 和 IPv6)，允许这些 RIR 作为证书颁发机构(Certification Authority，CA)为整个互联网数字空间的任何子集颁发一个证书。

每个 RIR 维护一个证书实践声明(Certificate Practice Statement，CPS)，描述了 RIR 向与主体实体(subject entity)的当前资源分配状态相匹配的主体颁发证书的实践。这些证书是证书颁发机构证书(Certificate Authority certificate，CA 证书)，CA 证书允许主体实体颁发更多的 RPKI 证书。当主体实体本身是执行数字分配的本地互联网注册机构(local Internet registry，LIR)时，

37 https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en

这些 RPKI 证书可以是 CA 证书；或者这些 RPKI 证书也可以是终端实体证书(End Entity certificate，EE 证书)，EE 证书的作用是认证生成数字签名的密钥。

由于证书本身是签名对象，从颁发者到主体的已颁发证书序列形成了一个认证路径，每个证书都由其颁发者签名。这个链的根是信任锚，信任锚是一个自签名证书。证书的验证需要形成一个连锁的颁发者/主体证书序列，该序列从信任锚开始，到被验证的证书结束。

RPKI 框架中的一类签名对象是路由源授权(Route Origin Authorization，ROA)对象。ROA 是一种可通过密码验证的声明，ROA 表明：“前缀 P(及其所有前缀长度不超过指定的最大前缀长度的所有子前缀)可以由自治系统号码(Autonomous System Number，ASN)A 声明，并签名：与前缀 P 对应的 IP 地址块的所有者。”在 RPKI 术语中，前缀 P 现在被一个 ROA“覆盖”。

可以有多个 ROA 覆盖同一前缀。最简单的例子是多宿主，其中一个前缀由两个(或更多)ISP 起源。第一个 ROA 将表示前缀可以由使用 AS 64496 的网络起源，而第二个 ROA 将表示同一前缀也可以由使用 AS 64497 的网络起源。另一个例子是一个 ISP 将一些地址空间从一个 ASN 转移到另一个 ASN。在一段时间内，这个地址空间将由两个 ROA 覆盖，一个用于旧的 ASN，一个用于新的 ASN。

如前所述，在发布 ROA 之前不需要获得 ASN 所有者的许可，甚至也不需要征求 ASN 的批准。尽管会发生这种情况(见章节 2.5.1)，但对于 IP 地址持有者来说，创建一个 ROA 来允许一个与其没有关系的 ASN 起源其前缀，最多只能说是一种值得怀疑的做法。

签名 ROA 的过程遵循传统的 X.509 签名流程。IP 地址块所有者创建一个自生成的私钥/公钥对和一个 EE 证书签名请求。该 EE 证书由所有者的 CA 颁发，并在 CA 的已签名附属产物的资料库中发布。IP 地址块所有者用私钥签名 ROA。然后，将组装一个包含 EE 证书、数字签名和路由起源证明(IP 地址块、最大前缀长度和起源 AS)组装成一个数字对象。这个数字对象就是准备发布的实际 ROA。随后将 ROA 放入 EE 证书中列出的发布点。

大多数 ISP 和大型网络可能有多个 IP 地址分配来源。并非所有这些地址块都来自同一个授权点。从多个来源接收地址的 ISP 需要运营多个 CA 证书，每个授权路径对应一个证书。

所有 CA 和 EE 证书都会到期。一般而言，到期时间与资源分配(allocation)或指派(assignment)有关的现行合同安排一致。在没有正式协议的情况下，RIR 们已经利用社区政策流程制定了一项约定的证书颁发策略。例如，在 RIPE 地区，这些证书的有效期为 18 个月。

2.3 RPKI：授权资料库与托管模型

RFC 7115[38]中描述的起源 RPKI 模型设想 RIR 们将向 LIR 和 ISP 颁发 CA 证书，这些 LIR 和 ISP 的实体将运行自己的证书和签名产物(如 ROA)的授权资料库。资料库结构在 RFC 6481 中描述[39]。资料库包含 CA 颁发的所有证书、ROA、一个证书吊销列表(Certificate Revocation List，CRL)和包含所有对象的一个清单。这种模型需要 LIR 和 ISP 在专业知识和运营能力方面进行大量投入。托管资料库的服务器必须 24/7 全天候维护。ICANN OCTO 最近用 RPKI 验证器软件进行的一项实验显示，许多 RPKI 资料库处于离线状态或数据过时。而且，直到最近，另一个关键的考虑因素是缺乏能够执行这些功能的高质量软件工具。

为了应对这些巨大的采用障碍，RIR 开发了一个托管模型。该模型最初用于引导系统启动，现在用于促进 RPKI 的采用。在这个模型中，每个 RIR 代表其 LIR 和/或成员托管一个证书和签名产品的大型资料库。因此，创建 ROA 的过程大大简化：LIR 和成员在其 RIR 的 web 服务器上访问自己的帐户，描述前缀和作为路由起源的 AS，然后单击“签名”。此模型中保留了颁发者和主体的严格 RPKI 结构，因此证书是并没有被改变，相对于许多零散的发布点组成的零散的证书基础设施，该托管结构要简单得多。

公平地说，授权模型更针对那些有运行密码学系统和管理证书经验，并且对在内部运行这些功能拥有信息和操作安全需求的组织。托管模型更适合于希望使用 RPKI 但不愿意或不一定能够在内部提高足够的密码专业知识的组织。

2.4 RPKI 起源验证：路由起源验证

RPKI 起源验证“路由起源验证”(ROV)是在 ISP BGP 对等点上的路由器使用的一个过程，该过程根据过滤器列表来自动地接受或拒绝 BGP 路由声明，而过滤器列表是根据 RPKI 和 ROA 预先生成的。参与的 ISP 被称为 RPKI 的“依赖方”，这是 X.509 PKI 社区的一个术语。

与其他安全 BGP 的方法相比，RPKI 起源验证模型的一个关键优势是相对容易采用(在本文 4.4 节中描述)，即在互联中执行 ROV 的路由器不需要验证 ROA 数字签名(形成和维护路由声明过滤器的先决条件)所需的 CPU 密集型密码学功能。目前大多数高端路由器都使用专用硬件来加速数据包的处理和转发。这些路由器上的 CPU 所完成的唯一重要任务是参与路由协议，并计算要下载到专用线路卡上的转发表中的路由表。因此，路由器往往有相当简单的通用处理器。

首先，BGP 路由器依赖运行验证器软件的外部计算机来执行密码学验证，并基于已验证的 ROA 构建前缀过滤器，并可能得到其他本地路由策略数据源的增强。然后，这些前缀过滤器使用

38 https://tools.ietf.org/html/rfc7115
39 https://tools.ietf.org/html/rfc6481

RFC 8210[40]中定义的 RPKI 路由器协议定期地与路由器同步，大多数路由器供应商已经实现了相应的 RPKI 逻辑，尽管最近在 APRICOT 2020[41]峰会期间组织的一次“deployathon”(大规模测试活动)发现至少一家主要供应商存在问题[42]。

验证器软件构造了一组所有前缀/授权 ASN 组合，这些组合是从验证器获得的任何有效 ROA 中提取的；这与按需进行的 DNSSEC 验证截然不同。为了执行这项任务，软件需要不断地与互联网上的所有 ROA 资料库同步。

建立这个列表的过程从下载五个 RIR 的 TAL 开始。TAL 可以在验证器软件中预先配置，也可以由网络运营商手动配置。一旦获得了 TAL，验证器软件就可以跟踪证书链中的发布指针，并从各种 RPKI 资料库中递归下载证书和签名的 ROA 产物。

本地知识可以添加到同步 ROA 列表中。RFC8416[43]中描述了如何做到这点的例子 “基于 RPKI 的 IP 地址本地化管理机制(Simplified Local Internet Resource Management with the RPKI，SLURM)”。一个简单的用例是 ISP 在其网络中使用专用 IP 地址(RFC 1918)[44]或专用 ASN(RFC 6996)[45]，并希望将 ROA 验证应用于这些网络和公用网络中。由于这些资源根据定义不是全球唯一的，因此不能由覆盖公共空间的 ROA 覆盖。RFC 6491 的第 5 节(描述了使用单个根的初始模型的操作)对此有一个说明。

一旦获得所有有效 ROA 的列表，下一步就是将对等路由器与验证器软件同步。如上所述，这是通过使用 RFC8210[46]中定义的 RPKI 路由器协议来完成的，现在这些对等路由器已经准备好对所有接收到的 BGP 声明使用前缀过滤器。

包含已声明前缀和起源 ASN 的 BGP 声明可归为以下三类之一：

- 有效：有一个匹配的有效 ROA(或者通过终止/撤销 EE 证书可以使 ROA 失效)，该 ROA 覆盖了声明中的前缀和起源 ASN，并且声明的前缀长度与 ROA 中指定的最大前缀长度兼容。
- 无效：有一个或多个 ROA 覆盖了该前缀，但起源 ASN 不同，或者所声明的前缀长度超过了 ROA 中指定的最大前缀长度。
- 未知：没有覆盖声明前缀的 ROA。

40 https://tools.ietf.org/html/rfc8210
41 https://2020.apricot.net
42 https://nsrc.org/blog/rpki_deployathon
43 https://tools.ietf.org/html/rfc8416
44 https://tools.ietf.org/html/rfc1918
45 https://tools.ietf.org/html/rfc6996
46 https://tools.ietf.org/html/rfc8210

目前一些网络运营商使用的被称为“拒绝无效”的 ROV 逻辑如下：

- 如果公告处于有效状态，则它被接受。
- 如果公告无效，将被拒绝。
- 如果未知(“NotFound”状态)，则接受。

逻辑的最后一部分对于最初优雅地过渡到 RPKI 起源验证世界是必要的。然而，对于“未知”或“未覆盖”前缀应该怎么做这个更困难的问题仍然没有答案。最后的结果可能是拒绝它们，但如何做到这一点仍然不清楚。RFC 7115[47]第 5 节中的当前建议是，“由于起源验证将逐步展开，覆盖范围将在很长一段时间内不完整。”因此，在存在“NotFound”的有效性状态下进行路由过滤应该持续很长一段时间。当前拒绝“NotFound”的网络运营商可能会将自己与大部分互联网分开。

这种带外 ROA 分发机制是一个重要因素，大大简化了 RPKI 起源验证的采用难度：不需要对 BGP 协议本身进行升级。然而，正如将在后面的章节中讨论的，带外传播机制并非没有问题。

需要注意，有时针对“RPKI 无效”这一术语会有一些混淆。“无效 ROA”是指其数字签名无法在 RPKI 中验证的 ROA，必须由验证器软件丢弃。“标记为无效的 BGP 声明”是一种 BGP 声明，这个 BGP 声明确实由有效的 ROA 覆盖，但是这些 ROA 都不匹配 BGP 声明中的起源 ASN(或最大前缀长度)，因此 BGP 发言者(speaker)可以丢弃这个 BGP 声明。

2.5 数据质量

ICANN 组织设置了两个 RPKI 验证器，RIPE 验证器[48,49]和 NLnet Labs Routinator[50,51]，并比较了两个验证器的输出。他们的输出结果 100%匹配。

在运行这些验证器时，出现了一些意外。在这里报道这些问题不是为了指手画脚，而是为了说明 RPKI 目前面临的一些问题。

应该记住，ROA 是可通过密码学验证的证明。以密码学的方式验证一个证明可以保证该证明已由声称其制作的一方的私钥签名。它不一定保证证明是客观真实的。

47 https://tools.ietf.org/html/rfc7115
48 https://www.ripe.net/manage-ips-and-asns/resource-management/certification/tools-and-resources
49 https://github.com/RIPE-NCC/rpki-validator
50 https://nlnetlabs.nl/projects/rpki/routinator/
51 https://github.com/NLnetLabs/routinator

2.5.1 不重要的起源 ASN

如前所述，ROA 由 IP 前缀的所有者签名，而不是由 AS 号的所有者签名。因此，完全可以在系统中插入不重要的 ROA，由地址块的合法所有者签名，但是以一些任意的 AS 号作为授权的起源 AS。

作者于 2020 年 2 月 26 日在运行验证器软件时发现以下 ROA：

ASN	前缀	最大前缀长度	起源 RIR
137519	103.118.18.0/24	24	APNIC
5	103.118.18.0/24	24	APNIC
11	103.118.18.0/24	24	APNIC
10	103.118.18.0/24	24	APNIC

WHOIS 检查显示，前缀 103.118.18.0/24 已由 APNIC 分配给孟加拉国的 Healthcare Pharmaceuticals，Ltd。AS137519 也被指派到孟加拉国的 Healthcare Pharmaceuticals，Ltd.公司，因此第一个 ROA 是预期的。然而，AS5 被指派给 Symbolics Inc.，一家总部位于美国马萨诸塞州的已倒闭的计算机制造商。AS10 被指派给位于马萨诸塞州的由 BBN Systems and Technologies Inc.托管的 CSNET 协调和信息中心。AS11 指派给马萨诸塞州的哈佛大学。作者联系了 103.118.18.0/24 网络管理员，试图了解后三个声明。结果是一个配置错误，在编写本文档时已被更正。

2.5.2 不同的最大前缀长度

在 2020 年 2 月 26 日另一组令人惊讶的 ROA 的例子是：

ASN	前缀	最大前缀长度	起源 RIR
8987	100.20.0.0/14	24	ARIN
14618	100.20.0.0/14	24	ARIN
16509	100.20.0.0/14	24	ARIN
16509	100.20.0.0/14	14	ARIN

前缀 100.20.0.0/14 和 ASN8987、14618、16509 都分配给 Amazon Inc。

对于前三个 ROA，Amazon 断言前缀 100.20.0.0/14 可以由 AS8987、AS14618 或 AS16509 起源。这些 AS 号都属于 Amazon。由于最大前缀长度被设置为 24，Amazon 还断言长度大于或等于 24 的任何 100.20.0.0/14 的子前缀也可以由同一个 ASN 发起。

但是，这四个 ROA 中的最后一个 ROA 的最大前缀长度设置为 14。它说明只有前缀 100.20.0.0/14 本身可以由 AS16509 起源。它还说明，任何子前缀都应该被拒绝。第四个 ROA 的不允许子前缀与第三个 ROA 的允许子前缀相矛盾。

目前，路由验证器被配置为接受与任何 ROA 匹配的任何前缀，实际上在所有 ROA 之间执行逻辑或。因此最后一个最大前缀长度为 14 的 ROA 将被忽略。

看上去这种配置有操作上的原因。作者联系了 Amazon，给出的解释是，这种情况是由于使用 ARIN 托管的 RPKI 工具集删除 ARIN 区域的 ROA 时出现的操作困难所致。较大的 ROA 将保留在系统中直到过期。

这个例子并不是唯一的，在引入更具体的 ROA 之后，保留与 RIR 分配的前缀长度相同的 ROA 已经成为一种相当普遍的做法。IETF SIDROPS 工作组目前的建议是，“只要可能，运营商应使用“最小 ROA”，只包括那些实际上起源自 BGP 的 IP 前缀，而不包括其他前缀。[52]”

有关最大前缀长度相关问题的更深入分析，请参见章节 4.2。

2.5.3 陈旧数据

在 Routinator 3000 RPKI 验证器的输出中发现了第三个操作问题的例子：

rsync://rpki-repo.registro.br/repo/HqatGkF4QDP6Set7UcbXnGGj2TkehDBZ24LGiaLAbd
zu/0/ABE2B87282296266F69CE04223629CFC8BFD6354.mft：stale manifest
rsync://rpki-repo.registro.br/repo/HqatGkF4QDP6Set7UcbXnGGj2TkehDBZ24LGiaLAbd
zu/0/ABE2B87282296266F69CE04223629CFC8BFD6354.crl：stale CRL
rsync://rpki-repo.registro.br/repo/DmyLDjMgaeUsYnfjUCfi8BYTx4tsZvsFPDws5wDs4x
Fa/0/AB06C1515EDB643DB9DF8E7E1361A8BB0683DE7A.mft：stale manifest
rsync://rpki-repo.registro.br/repo/DmyLDjMgaeUsYnfjUCfi8BYTx4tsZvsFPDws5wDs4x
Fa/0/AB06C1515EDB643DB9DF8E7E1361A8BB0683DE7A.crl：stale CRL

作者联系了注册机构.br。给出的解释是.br 成员正在使用 RPKI 授权资料库模型。在过去的某个时候，至少有两个成员建立了自己的资料库，但停止了对它们的维护。这些资料库现在处于脱机状态，导致与这些资料库关联的数据过时。

2.5.4 不良数据对 RPKI 的影响

52 https://tools.ietf.org/html/draft-ietf-sidrops-rpkimaxlen

虚假但可验证的 ROA 对运营的影响微乎其微。ROA 不是路由声明，因此上面讨论的虚假 ROA 不会将不希望的流量发送给受害 AS 或造成类似的伤害。然而，他们使签署了虚假的 ROA 地址块持有人产生路由泄漏的风险，如 2.5.1 节。因此，这个问题可以最好地描述为一个自我伤害，很可能是一个需要自我纠正的问题，对全球互联网几乎没有影响。还有一种情况是，潜在的攻击者获得对目标受害者的 RPKI 证书的控制权 - 可能导致发布这些伪造的 ROA - 然后进行与伪造的 ROA 一致的路由攻击。

然而，低质量的数据可能会给 RPKI 带来声誉风险。

2.6 ARIN 服务区域的 RPKI 和遗存(Legacy)地址

ARIN 通过注册服务协议向标准客户和遗存资源所有者(即在 RIR 存在之前被指派资源的实体)提供注册服务，其中传统资源所有者从 ARIN 获得基本注册服务，而不支付任何费用或签订合同(但只获得他们在 ARIN 成立时收到的服务)。ARIN 地区的一些遗存 IP 地址所有者已经签署了一份遗存注册服务协议(Legacy Registration Services Agreement，LRSA)[53]，有效地使他们成为 ARIN 的成员。然而，这些遗存 IP 地址持有者中的一些人迄今为止拒绝签订 LRSA，声称该协议将剥夺他们认为的一些权利。ARIN 拒绝向未签署 LRSA 的遗产持有人提供 RPKI 服务。由于大多数遗存地址都在 ARIN 区域内，许多遗存地址块无法被 ROA 覆盖。

RIPE 社区已指示 RIPE-NCC(向 RIPE 社区提供 RIR 和其他服务的组织)提供非成员服务合同[54]，以使遗存所有者能够使用 RPKI。RIPE 社区认为本合同的条款和条件比 ARIN 社区对 LRSA 更友好。因此，它对 RPKI 部署的阻碍较小。

虽然 RPKI 起源验证的采用率仍然很低，但 ARIN 的这个遗存地址问题并不是一个大问题。

2.7 资源 PKI 的其他使用

RFC7909[55]建议使用 RPKI 对路由策略规范语言(Routing Policy Specification Language，RPSL)对象进行签名。类似地，一些 RIR 中的一些政策建议已被采纳或正在讨论中，这些政策建议使用 RPKI 验证 IRR 中的数据并删除虚假条目。例如，请参阅 RIPE 的对象清理建议[56]。

如 4.4 节中所示，在路径验证方向上的新工作建议使用 RPKI。

53 https://www.arin.net/resources/guide/legacy/
54 https://www.ripe.net/manage-ips-and-asns/legacy-resources/ripe-ncc-services-to-legacy-internet-resource-holders
55 https://tools.ietf.org/html/rfc7909
56 https://www.ripe.net/publications/docs/ripe-731

IPv6 安全邻居发现(Secure Neighbor Discovery，SEND)也利用了 RFC6494 中的 RPKI[57]。

3 从 IANA 的一个根到五个(或更多)根

RPKI 的信任锚模型是随着时间的推移而演进的。这一演进对整个系统产生了影响。

3.1 起源模型：单根

2010 年互联网体系结构委员会(Internet Architecture Board，IAB)关于 RPKI 的建议要求使用一个单一的权威信任锚，该信任锚应该"与地址分配层次结构的根(现在是 IANA 功能的一部分)保持一致。[58]"

由于若干技术和政治原因，这一模型并未被实现。

从与国家基础设施自主控制相关的政治角度来看，对于 RPKI 是否有可能在美国(例如在 ARIN[59])托管一个或多个密钥的单一信任根的必要性进行了热烈地讨论。

从技术角度看，在将 ROA 覆盖的 IP 地址块从一个 RIR 转移到另一个 RIR 时，使用单个信任锚会增加一些复杂性[60]。由于证书无法路由到多个父级，此过程可能需要单根信任锚在转移过程中发挥积极作用，或者需要一个更复杂的间接级别的设置，设置中 RIR 可以证明他们将哪些资源转移到另一个 RIR。APNIC 最近的一篇博客文章包含了更完整的分析[61]。

2018 年，IAB 发布了一份新声明承认既成事实[62]。

3.2 用于 RPKI 起源验证的五份 RIR TAL

拥有五个独立的 RPKI 信任锚解决了政治问题。该系统基本上可以如最初设计的方式运行，即每个 RIR 只声明其控制的资源集所覆盖范围。当数字资源从一个 RIR 转移到另一个 RIR 时，这种操作仍然会在证书基础结构中产生复杂性。RIR 采用了一种稍微不同的方法，目标是减少证书基础设施的复杂性和相关的脆弱性。

57 https://tools.ietf.org/html/rfc6494
58 https://www.iab.org/documents/correspondence-reports-documents/docs2010/iab-statement-on-the-rpki/
59 https://www.arin.net/vault/participate/meetings/reports/ARIN_XXVIII/ppm1_transcript.html
60 https://tools.ietf.org/html/draft-rir-rpki-allres-ta-app-statement
61 https://blog.apnic.net/2020/04/21/rpki-and-trust-anchors/
62 https://www.iab.org/documents/correspondence-reports-documents/2018-2/iab-statement-on-the-rpki/

为了避免在 RIR 间转移 IP 地址块过程中赋予单个根一个积极的角色，RIR 部署了一个技术修复：每个 RIR 都凭借这一新的技术能力，声明覆盖整个地址空间和数字空间。这样，转移的地址块仍然可以(一段时间)被转出的 RIR 颁发的旧证书和转入的 RIR 颁发的新证书覆盖。
该技术为 RIR 简化了 RPKI 中的证书颁发和资源跟踪。他们没有列出曾经授权的完整 IP 地址块集，而是只列出覆盖整个 IPv4 和 IPv6 地址空间的前缀和所有 AS 号。

因此，RPKI 系统没有单一的信任锚，而是有五个这样的信任锚。这是互联网上的一个新情况，介于具有单个根的 DNSSEC 系统和具有数百个信任锚的 Web PKI 之间。

在多个根的情况下，现在可能会出现一些非故意导致的冲突 ROA(不属于 RIR 间 IP 转移的一部分)且他们来自不同的 RPKI 验证路径，而这些验证路径都是有效的。所有者和签名者现在可能是不同的实体。在大多数情况下，这不应该是一个主要问题；只要至少有一个 ROA 将路由对象分类为“有效”，那么其他 ROA 就会被忽略。但是，正如 5.5 节所述，这种情况仍然可能产生危害。这产生了三点观察：

- 协作是关键。协作如何实现，如何维持？
- 可能会产生冲突。如何检测和修复冲突？
- 一旦你有一个以上的 TAL，为什么将 TAL 的数量停留在 5？可以有任意数量的信任锚，正如我们已经看到的互联网路由注册库数量的激增。

3.2.1 RIR 协作

RIR 之间的协作是其业务的重要组成部分。例如，IP 地址块和 ASN 定期从一个 RIR 转移到另一个 RIR。转移的例子至少可以追溯到 2002 年，在早期注册转移(Early Registration Transfer，ERX)项目开始时[63]。IPv4 免费地址池的耗尽使得这种 RIR 间的 IP 转移更加频繁。RPKI 的更新和协作是正常转移过程的一部分。然而，RIR 在不断发展。如果 RIR 成为全球性组织，在“建立新的区域互联网注册机构的标准”[64]原则 1 中定义的现行模式将被改变，目前的技术合作水平是否会继续下去尚不清楚。

3.2.2 RPKI 冲突

尽管有最佳实践，冲突仍可能发生。如何检测到它们和如何修复它们仍然是一项正在进行的工作。RPKI 系统一定会受益于对 5 个数据库一致性的全局监测。

63 https://www.arin.net/vault/participate/meetings/reports/ARIN_X/PDF/erx.pdf
64 https://www.icann.org/resources/pages/new-rirs-criteria-2012-02-25-en

3.2.3 超过五个 TAL

RPKI 起源验证的验证器在处理 ROA 时不考虑 ROA 的来源。它们基本上对所有已验证的 ROA 执行逻辑“或”操作。因此，在 5 个 RIR TAL 之外添加另一个 ROA 数据源只是一个简单的配置问题。不受 RIR 控制的实体在颁发 RPKI 证书时可能不仅基于 RIR 注册数据，还基于信誉数据(或者完全其他的东西，例如遗存状态)。一个主要的例子是非常大的 IP 地址的所有者可能直接发布一个指向自己资料库的 TAL。

这种努力的成败取决于依赖方，即运行 RPKI 验证器的网络运营商。他们可以选择在验证过程中添加(或不添加)这些备选信任源的 TAL。如果有足够多的 Tier 1 网络和 IXP 开始使用这些数据源，那么可以想象未来会有更多的 TAL 进入验证器软件的默认配置中，就像 IRR 中已经发生的那样。

3.3 AS0：覆盖未分配空间

除了路由泄漏，还可以观察到另一个与路由安全相关的现象：IP 地址空间抢占(squatting)。本质上，这是一种一个 ISP 故意或非故意地声明未分配的 IP 地址空间的现象。这种现象通常会很快被检测到并得到修复，但在一段时间、几个小时或几天内，该地址块是连通的。IP 地址抢占经常被用来发动各种类型的攻击和滥用，例如发送垃圾邮件。

由于整个地址 IPv4 空间现在几乎全部分配完毕，人们可能会认为 IP 地址抢占问题在 IPv4 中发生的应该越来越少。然而，由于许多大型遗存的 IP 地址块没有被全部或部分地进行通告，IP 地址抢占问题可能仍然是一个值得研究的问题。

在 IPv6 中，由于只分配了一小部分地址空间，IP 地址抢占显然是一个安全威胁，因为无法获知谁在使用这个空间。

这个主题最初在 RFC6491[65]中介绍，它描述了 RPKI 的单个根的操作。文档中建议 IANA 对所有不打算进行路由的保留 IPv4 和 IPv6 资源颁发 AS 0 ROA。覆盖所有未分配地址空间的一组(或多组)特定 ROA 将需要由类似于最初单根模型中的单个实体颁发，或由每个 RIR 颁发一次。

APNIC 采用了一项新的政策提案，为所有 APNIC 未分配的前缀创建 AS0 的 ROA[66]。APNIC 的员工为实施该政策，将创建一个新的 TAL[67]，从而使 TAL 的总数达到 6 个。LANIC 正在讨论一个类似的提案(实现方案类似)，可能会使 TAL 的数量达到 7 个。RIPE 正在考虑一个类似

65 https://tools.ietf.org/html/rfc6491
66 https://www.apnic.net/community/policy/proposals/prop-132
67 https://www.apnic.net/community/security/resource-certification/#st-anchor

的策略，但实施方案不同[68]：未分配空间的列表将包含在一个由 RIPE-NCC 管理的 SLURM 文件中，该文件在带外可用并且不加密。在撰写本文时，ARIN 和 AFRINIC 均未考虑此政策。

除了增加 TAL，不同 RIR 采用的不同(和无法协作的)方法将在正确配置 RPKI 验证器软件时产生额外的复杂性。

为未分配的空间创建 AS 0 的 ROA 会产生其他后果，将在 5.6 节中进行了分析。

4 RPKI 技术问题

与任何技术，特别是与安全性相关的技术一样，RPKI 起源验证是建立在一系列技术选择上的，这些技术选择会产生影响。首先，X.509 是一个复杂的系统。尽管 RIR 托管模型使签名的部分变得相对容易，但授权模型保留了 X.509 的全部复杂性。最近的软件也大大简化了验证方的工作，但是实际操作仍然需要一定水平的专业知识，这些专业知识不一定在所有尝试部署 RPKI 的网络中都具备的。从 DNSSEC 的部署可以看出，即使这种密码学管理专业知识是在部署初期由热忱的工程师开发的，随着员工转移或轮换到执行其他任务，专业知识的水平通常会逐渐消失，并使维护流程和系统成为问题。

4.1 RPKI 可扩展性

RPKI 起源验证设计中选择不修改 BGP 造成的结果是，BGP 本身不能用于将 ROA 洪泛到验证器。取而代之的是，必须采用带外 ROA 分发机制，以使 RPKI 起源验证器软件能够访问其所需的数据。RPKI 选择的模型使验证器直接与所有 ROA 资料库同步。这是 RPKI 与 DNSSEC 的一个关键区别，在 DNSSEC 中验证 DNS 解析器按需执行验证：仅在需要时才下载(和缓存)必要的信息。

目前大约有 65,000 个 ASN，如果他们全部参与了授权资料库模型中的 RPKI 起源验证，则每个 RPKI 起源验证验证器将必须不断与 65000 个资料库保持同步，获知其中一些资料库可能处于脱机状态或无法访问。这意味着每天要进行 65000 x 65000 个连接，约 40 亿个连接要在全球范围内维护。这样的数据量导致完全同步可能无法实现，2012 年的一项研究表明同步时间可能超过 30 天[69]。

68 https://www.ripe.net/participate/policies/proposals/2019-08
69 https://pdfs.semanticscholar.org/f536/a85c49e8c9754b201b18610fd5b35bd70252.pdf

当前执行同步的协议是 *rsync*[70]。*Rsync* 的设计理念是最大程度地减少传输的数据量，其代价是在内存和 CPU 上占用大量资源。在 RPKI 起源验证的初期，这并不是一个重要问题，但现在随着采用率不断提高，这种局限性变得越来越明显：RIR 已指出同步时间可长达 24 小时[71]。

造成传播延迟的因素有很多。首先，必须更新相关的 ROA 资料库，并发布新版本的资料库。资料库发布以批处理的形式进行，发布间隔从几分钟到几小时不等。其次，RPKI 验证器需要更新其缓存，更新缓存同样是一个批处理过程，每个 RPKI 验证器按照其配置中指定的间隔进行更新。再次，BGP 路由器必须与他们关联的 RPKI 验证器同步，这可能也需要一些时间。

24 小时的传输上限与通常所说的“互联网速度”相去甚远。如果一个组织必须紧急更改其路由结构，那么这种长时间的的更新验证延迟可能会导致严重的运营问题。客观地说，降低路由系统操作的灵活性可能会给系统带来脆弱性。

目前正在部署一个基于 web 对象的新协议，RPKI 资料库增量协议 RRDP(RPKI Repository Delta Protocol)，RFC8182[72]，来逐步替代 *rsync*。RRDP 与 web 缓存相结合可以(在某种程度上)缓解上述的可扩展性问题。(因为我们处于 RRDP 部署的初期，所以这个期望尚待验证。)现在全面评估这一结论是否成立还为时过早，因为每个间隔为一小时(或更快)执行此同步的 ISP 的可扩展性问题都很大。随着路由对象数量的增加和 AS 数量的增加，RPKI 系统的可扩展性需求也随之提高。

在可扩展性问题中当前的缓解因素是，大多数签署其 ROA 的网络到目前为止都决定不采用授权 ROA 资料库模型，而是依赖 RIR 托管模型。例如，在 RIPE 区域中，只有两家选择了授权资料库模型：NLnet Labs 和 Randy Bush。在已广泛部署授权资料库模型的 APNIC 区域中，情况截然不同。在安全性方面，这种将关键安全功能外包的做法本身存在风险，但如 2.3 节所述，成本效益分析倾向于让除了最大和最精通密码学的 ISP 和 LIR 之外的所有 AS 使用托管模型。

与可扩展性问题相关的安全隐患也存在。第一个例子：RIR 受到攻击并为分配给 RIR 的地址前缀的完整集合生成 AS 0 ROA，然后撤销所有其他 ROA。第二个例子：任一 RPKI 发布点受到攻击，这个发布点似乎正在为 IPv6 前缀内的每个/128 IPv6 地址发布单独的 ROA。在这两种情况下，攻击者的意图都是将 RP 和资料库之间的同步工作洪泛到极大比例，从而导致整个 RP 软件停止工作。

4.2 最大前缀长度

70 https://rsync.samba.org
71 https://www.ripe.net/publications/docs/ripe-549
72 https://tools.ietf.org/html/rfc8182

当创建 ROA 时，除了前缀 X 和 ASN Z 之外，还有一个额外的参数 Y，即 ASN Z 能起源的前缀 X 的最大前缀长度 Y。让我们看一下运行 Routinator 3000 RPKI 验证器时看到的 ROA：

AS16509,100.20.0.0/14, 24, arin

第三个参数 24 表示 AS16509 可以起源 100.20.0.0/14 的任何子前缀，只要其前缀长度在 14 到(含)24 之间。参数还表示任何大于 24 的 100.20.0.0/14 子前缀都应被拒绝。

因此，例如由 AS16509 起源的 100.20.0.0/16、100.21.4.0/22 和 100.22.7.0/24 都应该接受，但应拒绝具有相同起源 AS 号 16509 的 100.22.7.4/28。

最初的建议[73]是设置最大前缀长度以匹配分配的地址块。如果得到/14 的前缀，则将最大前缀长度设置为/14。因为任何子前缀都会被自动拒绝，所以这样可以避免潜在的子前缀路由泄露。

这就产生了一些问题。例如，当网络运营商进行流量工程来响应流量事件或平衡多个链路上的流量时，特别是在 DDoS 攻击期间，常见的缓解方法是注入更多前缀更长的路由来转移部分流量。如上一节所述，由于 ROA 传播时间可能长达 24 小时，因此将 ROA 中的最大前缀长度设置为太短(*译注：原文为"太长"*)的值将导致无法快速响应事件。

因为无法预测地址空间的哪一部分将受到 DDoS 攻击，所以当前的操作实践是将最大前缀长度简单地设置为/24，导致最大前缀长度提供的初始防御效果被无效化了。(/ 24 是当前可在互联网上路由使用的最长前缀长度)但是，这会使地址所有者暴露于路由泄露场景的起源集合中。因为没有对 AS 路径的保护，所以攻击者可以将 ROA 中起源 AS 与 ROA 中前缀的更长子前缀合成新的路由，然后将这些子前缀的路由简单地注入到路由系统中。虽然这种攻击产生的(泄露的)AS 路径可能比真正的 BGP 通告更长，但是由于更长的前缀具有更高的优先级，并且 ROA 验证系统会将这些(泄露的)BGP 通告标记为有效，因此攻击将会成功。

4.3 RPKI 提供(或不提供)的保护

RPKI 起源验证通常作为一种工具，用来防止由于配置错误或蓄意攻击引起的路由事故。本节将分析 RPKI 起源验证对发现这两种事故的有效性。

4.3.1 非自愿错误

73 https://tools.ietf.org/html/rfc7115 章节 3

涉及路由误配置的事件分为如下几类：

- 打字错误(Typos)，又称为“胖手指失误(fat fingering)”。在大多数路由用户界面中，BGP 命令的句法相当容易出错，并且很容易(且经常)犯错误。内部检查不一定总能发现这些错误。
- 配置错误。配置 BGP 需要高水平的技能和专业知识，并且经常容易犯错。
- 软件中程序错误(bug)。路由泄露的一些最著名的根源来自有故障的软件，例如，带宽优化器软件将本地的路由泄露到互联网中。
- 实际上的恶意攻击。

通常的假设是前三种类型的泄露在每天看到的 BGP 路由错误起源事件中占大部分。实际比例很难确定，因为涉及确定泄露的意图(或缺乏泄露的意图)，而意图很难确定。本文作者无法找到任何数据来量化路由泄露的相对比例。

根据已发布的 ROA 参数，ROA 可能会阻止意外的路由错误起源。例如，在子前缀泄露的情况下，谨慎使用 ROA 最大前缀长度这一参数可能会使得子前缀被标记为无效，并被启用 ROV “无效拒绝”的 ISP 拒绝。但是，当前的做法似乎不这么使用最大前缀长度参数，因为这会阻止对网络通告进行紧急修改的能力。因此，目前尚不清楚 RPKI 起源验证实际上将阻止多少路由泄露。最近的研究调查了这一问题[74]。

正如 2.5.1 节中所举例说明的那样，还应注意，RPKI 起源验证不能防止 ROA 本身的配置错误。

4.3.2 攻击

通常认为，ROV 可以抵御某些依靠 BGP 泄露才能成功的攻击。

一个广为人知的攻击发生在 2018 年。攻击者使用 BGP 劫持将发送到 MyEtherWallet.com 权威 DNS 域名服务器的流量转移到攻击者控制下的一组域名服务器。不知情的 MyEtherWallet 的客户在几个小时内被重定向到一个伪造网站，攻击者在其中窃取了客户的凭据。估计有 1700 万美元被盗。如果名字服务器的前缀已受到 ROA 的保护，则该攻击可能会受到 ISP 部署 RPKI ROV 的限制。值得注意的是，如果 MyEtherWallet.com 已签名其 DNS 空间，则此攻击也将受到 ISP 部署 DNSSEC 验证的限制。

但是，ROV 不能抵挡稍微复杂的攻击。ROV 仅验证 BGP 通告的起源，不会验证路由通告的完整 BGP 路径。攻击者只需在 AS 路径前添加一个有效的起源 AS，即可转移流量。如果攻击

74 https://ripe80.ripe.net/presentations/14-3dleak_viz_madory_ripe.pdf

者以这种方式修改了自己的攻击，则 RPKI 起源验证不会阻止对 MyEtherWallet.com 发起的 BGP 攻击。

当在一个 AS 路径之前添加的 AS 是如此简单，人们只能得出如下结论，RPKI 起源验证只能保护免受最简单的攻击，而不能提供针对故意攻击的任何重要防御措施。值得注意的是，这种在 AS 路径前添加 AS 的做法可能会降低通告的“竞争力”，从而限制了通告的传播范围。但是，许多攻击故意没有在全球范围进行，而是在受限的环境(如 IXP)中进行。缩小范围不会对此类攻击造成太大影响。

4.4 路径验证之路

BGP 安全是一项复杂的工作。要完全做到这一点，需要验证路由通告中的完整路径，这已经被证明是一项非常艰巨的任务。

4.4.1 以前的尝试

过去已经进行了许多路径验证的尝试(并且被放弃了)。其中值得提及的包括：

- Secure BGP (sBGP)[75]。sBGP 最初于 2000 年被提出。其通过在 BGP 消息中前缀和 AS 路径上放置数字签名，提供了一种全面的方法来保护 BGP。这种方法在边界路由器上是 CPU 密集型的，并且需要修改 BGP 协议。该方法还容易受到降级攻击，这使其好处无效。
- BGPsec。BGPsec 是 sBGP 的演进，由 IETF 在 RFC 8205[76]中进行了标准化。它使用 RPKI 来存储有关 AS 间关系的数据。它具有与 sBGP 相同的缺点，因为它在路由器上是 CPU 密集型，需要修改 BGP，并且难以增量部署。
- Secure Origin BGP (soBGP) [77]。soBGP 互联网草案的最新更新时间是 2006 年。soBGP 与 RPKI 一样，专注于 AS 起源验证，但通过经过认证的 AS 邻接关系添加了 AS 路径是否合理的测试。关于 soBGP 的工作比 RPKI 早了很多年，该提案的设计者选择使用以信任网络作为基础，但这并不是 soBGP 的基本方面，soBGP 也可以很容易地使用 RPKI 来代替信任网络。IETF 多年来致力于解决应用于路由对象传播(AS 路径验证)的严格测试与 soBGP 中使用的 AS 路径合理性概念之间的区别。注意：soBGP 还将需要对 BGP 协议进行修改。
- Inter-Domain Route Validation(IRV)[78]。IRV 最初于 2003 年发布。与 RPKI 起源验证类似，且与上述两种方法相反，IRV 不需要修改 BGP 协议，而是使用带外验证的方法。IRV 基于

75 Seo, K., S. Kent, and C. Lynn, "Secure Border Gateway Protocol (Secure-BGP)", IEEE Journal on Selected Areas in Communications Vol. 18, No. 4, April 2000, pp. 582-592.
76 https://tools.ietf.org/html/rfc8205
77 https://tools.ietf.org/html/draft-white-sobgp-architecture-02
78 http://patrickmcdaniel.org/pubs/ndss03.pdf

以下想法：AS 应负责维护其起源或提供中转的所有前缀的数据库(类似于 IRR)。验证路由器可以使用 IRV 协议查询起源 AS 的 IRV 数据库以执行起源验证。IETF 从未对 IRV 进行过全面探索或分析。

4.4.2 缓解方法

如今，路径验证仍然是一个遥不可及的目标。可以采取部分缓解措施如下：

- 增加直接对等(peer)关系的数量。使用直接对等时，路径是单跳，因此路径验证在逻辑上等效于路由起源验证。
- 同样，AS 路径越短，AS 路径攻击成功的可能性就越小。
- 使用内容分发网络(CDN)或缓存使内容更接近终端用户，这将对缩短 IP 级 AS 路径起到应用级的作用。
- Peerlock[79]是 AS 路径过滤的一组经验方法，可以防止大量泄漏。例如，它观察到出现在 AS 路径中无需中转(transit-free)网络(Tier 1)不应超过两个。因此，应过滤掉包含两个以上 Tier 1 的 BGP 通告。

只有通过使用 ROA 中尽可能最短的最大前缀长度来阻止注入子前缀的路由，缩短 AS 路径的缓解方法才能生效。但是，这会带来其他问题，如 4.2 节所述，并且与当前建议中的将最大前缀长度设置为 24 的做法相冲突。

单独或集体部署这些技术都无法解决路径验证的问题。它们可能会缓解一些配置错误和软件错误，但是这些措施都无法提供任何现实形式的安全防御。

那么就合理地提出一个问题：RPKI 起源验证是否是这条路的尽头？在可预见的将来，路径验证是否遥不可及？

4.4.3 新提案：ASPA

IETF SIDROPS 工作组不断提出有关如何解决路径验证问题的新想法。值得一提的想法是对 RPKI 的自治系统提供者授权(Autonomous System Provider Authorization，ASPA)扩展[80]。

ASPA 利用了 soBGP 的一些关键思想，即 AS 路径合理性。这里的关键点是，不需要全面和完整的路由保护-目的是限制 AS 路径中无法检测到的一组谎言。建议的路径验证过程不需要修改 BGP 或处理 BGP 更新，而是依靠新的 RPKI 对象 ASPA 创建和分发 ISP 级 C2P 关系的数据库。ASPA 相当于 ISP 的 ROA。它证明“客户 AS 所有者(Customer AS holder，CAS)已

79 https://archive.nanog.org/sites/default/files/Snijders_Everyday_Practical_Bgp.pdf 和 https://youtu.be/CSLpWBrHy10
80 https://tools.ietf.org/html/draft-ietf-sidrops-aspa-verification

授权特定的提供商 AS(Provider AS，PAS)传播客户的 IPv4 / IPv6 公告。”就像 soBGP 一样，由于 ASPA 是 AS 级粒度的授权，因此 ASPA 不能为路径验证问题提供完整的解决方案。ASPA 无法保护具有正确 AS 关系的非故意的路由泄漏。但是，与 BGPsec 相比，ASPA 的相对简单性可能使其对路由器供应商和网络运营商更适合。

基于 RPKI 的 ASPA 共享 RPKI 起源验证的某些属性。它对边界路由器的 CPU 影响比较低，并利用现有的 PKI 和管理工具，有效地减少使用上的障碍。相反地，ASPA 也继承了与 RPKI 模型相关的风险，例如 X.509 模型十足的复杂性，分布式资料库模型的可扩展性问题以及由于五个根之一的违规行为而可能造成的灾难性场景。

5 RPKI 操作风险

RPKI 起源验证系统带来许多需要考虑的操作风险。这些“不良影响”的分类法可以在 RFC 8211 中找到[81]。

5.1 意外拒绝有效路由

路由起源验证会带来一种固有风险——误报，即拒绝真实的路由，因此会丢弃客户的流量。ROV 逻辑着重于寻找可以覆盖前缀的任何 ROA。在大多数情况下，被污染的 ROA 不应带来误报。但是，在某些情况下，如果针对一个被 ROA 覆盖的聚合缺少子前缀声明的 ROA，或者针对先前未发现的前缀存在被污染的 ROA，则可能导致误报。

许多 ISP 和 IXP 测试了“拒绝无效”ROV 逻辑，并观察到，尽管被 RPKI 判定为无效的 BGP 通告数量仍然很重要(大约 1%)[82]，但流向这些前缀的实际流量非常小[83]。这种观察已说服那些运营商打开自动声明过滤。宣布其 ROV 计划的 ISP 包括：NTT[84]，AT&T[85]，Telia Carrier[86]，Orange IC[87]和 Seacom[88]。其他许多运营商正在部署 ROV“拒绝无效”，但尚未公开宣布其计划。在 IXP 方面，阿姆斯特丹 IX(AMX-IX)[89]，DE-CIX[90]，西雅图 IX[91]和卡尔加里 IX(YYCIX)[92]正在部署“拒绝无效”ROV。

81 https://tools.ietf.org/html/rfc8211
82 https://observatory.manrs.org/#/overview
83 https://blog.benjojo.co.uk/post/the-year-of-rpki-on-the-control-plane
84 https://www.us.ntt.net/support/policy/rr.cfm#RPKI
85 https://mailman.nanog.org/pipermail/nanog/2019-February/099501.html
86 https://www.teliacarrier.com/Our-Network/BGP-Routing/Routing-Security-.html
87 https://twitter.com/OrangeIC/status/1233013893771005952
88 https://www.ripe.net/participate/mail/forum/routing-wg/PDZlMzAzMzhhLWVhOTAtNzIxOC1lMzI0LTBjZjMyOGI1Y2NkM0BzZWFjb20ubXU+
89 https://www.ripe.net/support/training/ripe-ncc-educa/presentations/use-cases-stavros-konstantaras.pdf
90 https://www.de-cix.net/en/resources/route-server-guides/rpki
91 https://www.seattleix.net/route-servers
92 https://yycix.ca/communities.html

重要的是要记住，这些观察反映了 RPKI 部署的当前状态。它仍处于初期阶段，并非所有前缀都包含在 ROA 中。截至 2020 年 2 月 28 日，有：

- 112,848 个 IPv4 ROA，涵盖 104,369 个唯一的 IPv4 前缀。该数据是从 Routinator 中提取的。多个 ROA 可能覆盖相同的前缀，或者具有不同的起源 ASN(例如，多宿主)或具有不同的最大前缀长度。
- RIR 共作出了 210,754 个 IPv4 指派。此数字是从 NRO 授权扩展的统计信息中收集的[93]。
- BGP 中声明了 822,085 个 IPv4 前缀[94]。历史上，BGP 中的前缀数量一直是 RIR 分配的块数量的几倍。这主要是由于 ISP 的流量工程实践，通常会分解前缀并将其声明为更长前缀。
- 18,956 个 IPv6 ROA，涵盖 17,322 个唯一的 IPv6 前缀。
- RIR 作出了 49,476 个 IPv6 指派。
- BGP 中声明了 47,074 个 IPv6 前缀。

以上统计数据表明，RPKI 在 BGP 通告数量中的全球普及率在 IPv4 中约为 14%，在 IPv6 中约为 40%。

要记住的另一点是，由于误报导致的少量流量丢失的观测是在最佳情况下进行的。如果在 RPKI 系统中发生重大事件(请参阅 5.5 节)，那么很可能会丢失流量。尚有待解决的问题是丢失多少流量，可能造成什么损害，如何检测到这种损害以及如何迅速修复。

与此相关的还有一个未解决的问题：ISP 是否可以依靠第三方管理的数据来做出关键的业务决策，即使该数据是经过密码学签名的？到目前为止，许多 ISP(例如 ATT，NTT 等)和企业(例如 Cloudflare 等)在 RPKI 失败的潜在风险与路由泄漏、软件错误和配置错误之间权衡，都已经决定值得部署 ROV。其他网络运营商仍在等待更具吸引力的案例来激活这种形式的路由过滤。

5.2 自我断开

在为网络配置 ROA 时，经验不足的工程师在使用其 RIR 管理 RPKI 的门户时可能会面临一个特殊的风险：只将前缀和没有关系的 AS 进行关联。例如，网络工程师可以创建单个 ROA，授权 AS 0 声明其网络前缀。由于此 ROA 会传播到部署 RPKI 起源验证“拒绝无效”的各个网络，因此该网络的前缀将停止在互联网上传播。在那时，工程师可能很难解决此问题：他们可能无法再连接到 RIR 服务器以更正配置。

5.3 可用性风险：停机

93 https://www.nro.net/about/rirs/statistics/
94 https://www.cidr-report.org/as2.0/#General_Status

依赖方(在其 BGP 输入上执行 ROV 的网络)需要维护 RPKI 中所有有效已发布材料(所有证书、所有当前 CRL 和所有已发布的签名产物)的本地缓存。此过程依赖于与所有 RPKI 发布点的定期同步。因此，发布点的持续可用性是必需的。这些资料库离 RPKI 根目录越近，它们的可用性就越关键。

尽管付出了最大的努力，但停机还是发生了，其中值得关注的是：

- RIPE-NCC 于 2013 年 2 月 3 日长时间停机[95]；
- ARIN 于 2018 年 10 月 24 日长时间停机[96]；
- APNIC 于 2019 年 12 月 13 日停机[97]；
- AFRINIC 于 2020 年 3 月 30 日停机[98]；
- RIPE-NCC 在 2020 年初发生了四次停机(最受关注的一次是在 2020 年 4 月 6 日) [99]。

最近有两次 RIPE-NCC 停运值得探讨以从中得到教训。2020 年 2 月 22 日停机[100]的根本原因是未监视的磁盘分区超过其配额。这导致 RIPE 资料库的一部分，即证书召回列表(CRL)过期。该过期触发了多个依赖方的级联效应。对于某些人来说，RPKI 验证器软件会使整个资料库无效。对于其他人，他们的验证器软件什么也不做，或者只是发出警告。该事件在 SIDROPS IETF 工作组中引发了关于验证器软件的正确行为的讨论。2020 年 4 月 6 日停机的根本原因是系统集成问题，其中一个组件向正处于维护窗口中的另一个系统进行查询。这导致了丢失数据，恢复数据花费了数个小时。

通常情况下，在 RPKI 发布点无法访问的情况下，依赖方应使用其本地缓存。具体来说，情况更加复杂。超过下次更新时间(已过期)的 CRL 的不可用性给依赖方带来了一个难题。他们是否应该在知道信息已过期的情况下继续应用过期的本地缓存的 CRL 吊销信息，还是宣布此发布点的整个本地缓存无效？(在 RFC 8767[101]中讨论了 DNS 世界中的相似之处)不应将 CRL 和清单陈旧性与数据过期混淆。陈旧性意味着数据的发布者已经告诉你现在要进行另一次更新，但尚未到来。它不会自动使任何数据无效。对于已过期的本地缓存证书，情况有所不同。不应在 RPKI 验证过程中使用已过期的证书。

只要 CA 使用一种证书刷新实践方案，该实践会在证书到期前刷新证书，短暂的停机就不会出现运营问题。持续超过一天或几天的长时间停机可能会带来更明显的运营问题。在大多数情况下，结果只会是 ROA 不再覆盖某些前缀。在验证过程中，它们将被标记为“未知”状态。ISP 对

95 https://www.ripe.net/support/service-announcements/service-announcements/ripe-ncc-rpki-repository-outage
96 https://www.arin.net/vault/announcements/2018/20181024.html
97 https://www.apnic.net/about-apnic/service-updates/service-announcement-13-december-2019/
98 https://lists.afrinic.net/pipermail/rpki-discuss/2020-March/000108.html
99 https://www.ripe.net/support/service-announcements/rsync-rpki-repository-downtime
100 https://www.ripe.net/ripe/mail/archives/routing-wg/2020-February/004015.html
101 https://tools.ietf.org/html/rfc8767

“无效”进行过滤不会产生任何后果。但是，在某些情况下可能会出现问题。一个例子是前缀基于最大前缀长度匹配的原因被一个 ROA 覆盖，而且存在其他 ROA 以更长的子前缀覆盖此前缀。如果较长前缀覆盖的 ROA 消失了，但聚合的前缀 ROA 仍然保留，则较长前缀覆盖的 ROA 匹配的路由将被标记为“无效”，因此被拒绝。另一种情况是，依赖方(无意间或以其他方式)最终在 RPKI 系统中过滤了前缀“NotFound”。有关拒绝“NotFound”的讨论，请参见 2.4 节。

鉴于以上所述，RPKI 发布点的运营管理过程应被视为一项关键业务活动，依赖方对 RPKI 数据的恰当利用也是如此。

5.4 一致性风险：五个或更多信任锚

五个自签名证书的“重叠”信任锚集，其中每个证书列出了整个 IP 资源集，导致一种潜在的情况，即配置错误可能导致两个(或多个)RIR 发布不一致的信息。这也意味着，如果针对单个 RIR 的 RPKI 发布系统的一个成功的攻击被实施，则攻击者可能会发布任何数字资源的 RPKI 材料，而不仅仅是 RIR 管辖范围内的数字资源。

考虑到 RIR 的运营可靠性，这似乎是极不可能的情况，但是，值得关注的一个特殊情况是，如果向 RIR 提出法院命令或其他政府授权，要求 RIR 单方面更新其数据库，将会发生什么情况？例如，要求的目标是关闭某个国家/地区的网络。

下一节将分析这种一致性风险的潜在后果。

5.5 完整性问题：违规

更令人担忧的情况是一个 RIR 上的安全性违规。

5.5.1 潜在的故障场景

这种情况可能是由于软件错误、被攻破的员工或对 RIR 基础结构的直接攻击而发生的。以下是可设想的灾难性故障场景的例子：

- ROA R 涵盖了关键服务/基础架构提供商(甲方)使用的地址。
- 主要的 Tier 1 中转 ISP 们部署了自动 ROV。
- 持有 ROA R 的一个 RIR 是安全漏洞的受害者，攻击者控制了该 RPKI RIR 资料库。
- 攻击者想对甲方造成伤害。
- 攻击者撤消了用于签署 ROA R 的有效证书，并针对不同的(可能不存在的)起源 ASN 发行了新的有效证书并签署了新的 ROA R2。

- 由于缺乏系统的监控，证书和 ROA 变更会传播到依赖方，并且可能很长一段时间都不会被发现。
- RPKI ROV 保持运行而不会发出警报(所有其他证书看起来都没问题)。
- 使用自动 ROV 的所有 ISP 丢弃来自甲方的路由通告。
- 甲方变得无法从互联网的大部分区域访问，这可能会影响依赖于甲方的系统。

这种情况不容易检测或处理。除了被黑掉的前缀外，其余的 ROV / RPKI 基础结构仍保持正常工作。破坏生效之前该问题不太可能会被发现。

5.5.2 复原

一旦发现问题并引起受攻击的 RIR 注意时，RIR 将修复安全漏洞并颁发新的证书和新的 ROA。这个过程肯定会花费时间。5 分钟至 24 小时的 RPKI 传播时间肯定会是一个加剧伤害的因素。在此期间，所有 ISP 都有可能关闭 ROV。

在此场景的变体中，由于有五个 RIR RPKI 根，因此在任何 RIR 上的任何违规行为都可能对所涵盖的 ROA 产生影响。攻击者控制一个 RIR 的 RPKI 系统，也可能对其他 RIR 的 IP 地址块中的前缀造成损害。验证器软件通常会在所有 ROA 之间执行逻辑或，因此重复但矛盾的 ROA 不会直接导致任何网络离线。但是，这种场景可能产生路由泄漏的隐患。特别地，这能允许一个精心设计的路径“无处泄漏”从而有效地将一个网络下线。

5.5.3 变化

另一种场景也会影响不使用 RPKI 且没有 ROA 的组织。任何 RIR 的破坏都可能使攻击者将这种组织从互联网上移除，攻击者只需通过为目标前缀发出与 ASN 0 关联的虚假但有效的 ROA。在这种情况下，就不需要向 BGP 注入虚假信息了。添加伪造的 ROA 就可以将现有的真实 BGP 路由对象标记为无效。

任何 RIR 上的任何违规行为都可能对 ROA 覆盖或不覆盖的前缀造成各种损害。下表总结了这种情况：

	签署前缀的 RIR 的违规行为	其他 RIR 的违规行为
ROA 覆盖的前缀	前缀离线	可以通过更多细节来解决路由泄漏问题，这可能会导致前缀的一部分或全部离线
ROA 不覆盖的前缀	前缀离线	前缀离线

可以将这种情况与单根系统进行比较。根的违规可能会删除任何前缀，但是任何 RIR 的违规只会影响其指派/分配的前缀。

	根的违规行为	签署前缀的 RIR 的违规行为	其他 RIR 的违规行为
ROA 覆盖的前缀	前缀离线	前缀离线	无
ROA 不覆盖的前缀	前缀离线	无	无

但是，还有另一点需要观察：如果 RIR 违规，受到损害或受到法院命令，则五信任锚系统可能会提供恢复的途径。其他四个 RIR 可以开始向受影响的各方签署 CA，以便他们可以签署其 EE，从而签署其 ROA。此时，依赖方可以删除受影响的 RIR 的 TAL。这将部分地缓解该问题，但肯定会花费一些时间来实施。

总而言之，让五个根中的每一个都声称覆盖整个 IP 地址空间的决定，增加了攻击面和任意 RIR 违规的后果。相对的，它为发生违规情况提供了一个潜在的(尽管很慢)恢复的途径。

5.6 RPKI 导致的 RPKI 资料库可达性损失

如果 ROA 分发机制受到攻击，或者依赖方收到的 ROA 在传输过程中被破坏，则到达 RIR 管理的 ROA 资料库之一(或其下的一个委托资料库)的路径可能会失效，后果是资料库将不可达。

如果 RIR ROA 资料库变得不可达，则可能会很快检测到该问题。但是，可能需要花费更多时间来检测(并修复)位于链下游的被授权的资料库的问题。(2.5.3 节给出了来自一个被授权的资料库的陈旧数据的示例)。在没有监视系统扫描发布点是否“活跃”的情况下，没有人可以确定这种情况是否已经发生。目前还不清楚如何从这种情况下恢复操作。可能需要手动干预才能恢复丢失的路径。显然，这种干预属于经验丰富的操作员(精通于密码学系统管理，尤其是 RPKI 的管理)所能做的事情的范围，但是经验不足的操作员处理该场景时可能会遇到更多困难。

5.7 路由策略

一个关键的问题是，当 RIR 成员拖欠费用并停止支付其注册费时会发生什么。在 RPKI 之前，RIR 将收回 IP 地址块并使关联的反向 DNS 条目无效。这有可能会立即影响违规成员网络的运行。但是，使用 RPKI 会使 RIR 的权力更大。现在，他们可以使该成员的 CA 失效，从而使其所有 ROA 失效。例如，RIPE 已经这么做过[102]。由于当前预期的 ROV 策略是接受“RPKI NotFound”的路由，因此这种 RIR 故意撤销的行为造成的影响效果仍然有限。

102 https://www.ripe.net/publications/docs/ripe-716

但是，如果违规成员的 RIR 实施了 3.3 节中所述的 AS 0 之类的策略，则会为相应的前缀创建与 AS 0 关联的新 ROA。这样做的结果是在 24 小时的 RPKI 传播延迟窗口内，使违规成员网络脱离互联网。为了纠正这种情况，网络运营商将必须使用带外机制来联系其 RIR，因为其网络连接将被暂停。

关于互联网的著名说法之一是没有路由警察。RPKI 起源验证在某种程度上使 RIR 发挥了部分路由警察作用。至少，它使 RIR 在路由系统的日常活动中发挥了新的关键作用。RIR 可能已经或可能没有为该角色做好充分准备。

5.8 RIR 支持模型

RPKI 向 RIR 施加的这一新角色给 RIR 带来了高风险，因此每个 RIR 所提供的运营支持水平至关重要。RIR 确实为托管 5 个 RPKI 根的系统提供了 24/7 联系支持，但是 RIR 的“联系我们”页面上未列出如何与 RIR 联系以解决紧急 RPKI 问题。在所有情况下，RIR 应该发布星期一至星期五，7 点到 7 点或 9 点到 5 点(在 RIR 所在的时区)支持的联系信息。RIR 的联系信息：

- AFRINIC: https://afrinic.net/contact
- APNIC: https://www.apnic.net/about-apnic/organization/contact-apnic/
- ARIN: https://www.arin.net/contact/
- LACNIC: https://www.lacnic.net/630/2/lacnic/contact-us
- RIPE-NCC: https://www.ripe.net/support/contact/technical-emergency-hotline

在一项最近进展中，ARIN 现在在其网站的每个页面底部包含一个指向“报告服务问题”的链接。

尽管 RIR 自然地处在声明有关地址块所有者的信息的位置，但 RIR 社区可能需要评估他们是否愿意确保其 RIR 拥有必要的资源和职权范围，以确保其 RIR 是一个运营路由控制系统的根的恰当地方。

5.9 SLURM

除了章节 2.4“使用 RPKI 简化本地互联网资源管理(Simplified Local Internet Resource Management with the RPKI，SLURM)”中介绍的处理本地专用网络的简单用例之外，RFC 8416[103]的开发还具有更大的目标：创建本地覆盖功能，以保护路由免受 RFC 8211 中所描述的不利行为的影响[104]。

103 https://tools.ietf.org/html/rfc8416
104 https://tools.ietf.org/html/rfc8211

依赖方的管理员可以创建以 json 格式表示的 SLURM 文件，列出许多本地例外，以覆盖来自 RPKI 的数据。此文件在创建 BGP 通告过滤器时由验证器软件处理。

第一个要问的问题是，管理员除了 2.4 节中提到的本地知识信息以外，如何确切地知道将什么放入 SLURM 文件中。在发生重大 RPKI 事故时的运营模型尚不清楚。是否会分发一个 SLURM 文件？由谁分发？如何对其认证？如何将其撤销？如果社区希望大规模使用 SLURM，那么这些问题召集对 SLURM 部署指南和操作模型进行进一步细致讨论。

来自不同来源的若干 SLURM 文件或许需要被合并。RFC 8416 中 4.1 节解释了一个 SLURM 文件的应用必须是原子的，即该文件中包含的所有断言必须都经过验证，该文件才能被考虑。4.2 节解释说，不同的 SLURM 文件之间应该没有冲突，如果有冲突，则必须丢弃整个 SLURM 文件集合。以上两个注意事项将确保本地的断言数据库的完整性，但会带来运营挑战，令 SLURM 的使用变得脆弱。

6 RPKI 责任问题

RPKI 依赖方们可能是，也可能不是，一个或多个 RIR 的成员，但是没有依赖方是所有五个 RIR 的成员。然而，所有依赖方都需要来自所有五个 RIR 的 RPKI 数据来执行一个完整的 RPKI 起源验证 ROV。因此，RIR 发现自身处于需要向先前无正式关系的非成员提供服务的位置上。

为非成员提供服务对于 RIR 而言并不新鲜。例如，所有 RIR 都已发布 WHOIS 数据多年。新鲜的是，通过使用 RPKI ROV，ISP 现在可以直接使用 RIR 的 RPKI 数据来进行过滤和路由决策，并且 RIR 现在已嵌入路由系统的关键路径中。由于存在这种实时依赖性，使用 ROV 所涉的风险要比发布 WHOIS 数据高得多。如果 RIR 犯错、被黑客入侵或长时间停机，则可能会对第三方造成重大损害。同样，以当前最佳实践(例如，部署策略以拒绝 RPKI“未知”路由通告)之外的方式使用 RPKI 数据并遭受直接或间接中断的依赖方可能会起诉产生该数据的 RIR。在北美地区，ARIN 已将这种情况视为主要责任风险和对 ARIN 组织的生存威胁，必须予以缓解。所选择的缓解方法是要求所有使用 ARIN RPKI 数据的依赖方对使用 ARIN RPKI 数据造成的损失免责。

6.1 ARIN 特定法律和技术方法

ARIN 已经建立了一系列机制来保护自己免受 RPKI 故障引起的责任。

6.1.1 ARIN 依赖方协议

ARIN 已创建依赖方协议(Relying Party Agreement，RPA)[105]，使用 ARIN TAL 进行 RPKI 验证的任何人都必须接受该协议。为了迫使用户同意 RPA，ARIN TAL 不能随意地获得，而是用户必须在一个称为“browseware”的过程中导航到一个网页。

根据宾夕法尼亚大学法学院的 Christopher S. Yoo 进行的研究[106]，“browseware”过程是一种有效的法律工具，可以保护 ARIN 免受其应负的责任，并且可能是这样做的唯一可行的方法。但是，同一项研究得出的结论是，ARIN 的 RPA 构成了进入 RPKI 的重大障碍。依赖方可能会或可能不会愿意因使用 RPKI 数据而对 ARIN 进行免责。即使他们愿意，他们也可能会面临内部挑战，很难或有时甚至无法同意 RPA。(例如，以上论文提到，政府实体可能被禁止同意免责、仲裁和法律条款的选择。尝试部署 RPKI 的非政府实体网络工程师不得不让其法律部门进行审核、理解和批准 RPA)这一最后步骤可能不是阻碍进一步发展的障碍，而是影响平衡的障碍。研究发现，最终结果是在五个 RIR 中 ARIN 地区的 RPKI 部署量最少。

最近的一份数据在路由起源验证一侧确认了这一点。2020 年 2 月 2 日，一个 RPKI 监控器[107]仅列出了北美地区使用 RPKI ROV 的少数实体。但是，签署 ROA 并不需要同意 ARIN 的 RPA。2020 年 2 月 28 日在一个 RPKI 验证器上看到如下数据：

	ARIN	RIPE	APNIC	LACNIC	AFRINIC	Total
IPv4 ROAs	7,494	68,674	29,440	6,399	841	112,848
ROA 覆盖的唯一的 IPv4 前缀	6,493	63,436	27,679	5,937	824	104,369
分配的 IPv4 地址块	64,235	81,368	44,097	17,321	3,733	210,754
ROA 覆盖的已分配 IPv4 占比	10%	78%	63%	34%	22%	50%

105 https://www.arin.net/resources/manage/rpki/rpa.pdf
106 https://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=3037&context=faculty_scholarship
107 https://rov.rpki.net

	ARIN	RIPE	APNIC	LACNIC	AFRINIC	Total
IPv6 ROAs	1,348	9,824	6,150	1,487	147	18,956
ROA 覆盖的唯一的 IPv6 前缀	1,258	9,412	5,166	1,340	146	17,322
分配的 IPv6 地址块	7,117	21,190	10,207	10,032	930	49,476
ROA 覆盖的已分配 IPv6 占比	18%	44%	51%	13%	16%	35%

根据这些数据，可以认为，与 RIPE 和 APNIC 区域相比，ARIN 区域普遍对 RPKI 缺乏兴趣，无论 ARIN 的 RPA 责任问题如何。

ARIN RPA 的另一个可观察到的结果是，大多数 RPKI 验证器软件并未预先配置 ARIN 的 TAL。依赖方必须采取额外的手动步骤来同意 ARIN 的 RPA，下载 ARIN 的 TAL，然后在验证器软件上进行配置。结果许多依赖方仅使用来自其他四个 RIR 的数据。

ARIN 确实允许验证器软件供应商拥有安装工具，这些安装工具可在用户同意 RPA 之后获得并安装 ARIN TAL。但是，一些软件供应商认为这使他们处于代表用户对 ARIN 免责的境地，他们不愿承担此责任。NLnetLabs Routinator 3000 和 RIPE Validator 仍然需要额外的手动步骤来安装 ARIN 的 TAL。

6.1.2 ARIN 的不可抵赖方法

除 ARIN 之外，采用托管 RPKI 模型的 RIR 成员只需登录其帐户即可生成 ROA。RIR 持有证书，以代表其成员签署 ROA。ARIN 对托管 RPKI 系统的设计有所不同。ARIN 不保留用于代表成员生成 ROA 的密钥。ARIN 成员需要使用自己的私钥通过 SSL 登录到 ARIN 的门户，然后使用自己的密钥生成 ROA。ARIN 的服务器上没有成员密钥，为 ARIN 组织提供不可抵赖性：即使 ARIN 的几名员工被攻破，他们也无法代表成员签署 ROA。同样，即使法院或国家政府下令，这种不可抵赖性也会阻止 ARIN 创建 ROA。不利的一面是，用户需要管理自己的公/私密钥对才能登录系统(这与在其他 RIR 中仅使用密码不同)。这意味着在 ARIN 区域中创建 ROA 比在其他区域中更为复杂。更重要的是，尽管 ARIN 的方法确实降低了 ARIN 的内部人员可能创造(由资源所有者)未经授权的 ROA 的风险，但这种操作方式上的转移却为用户增加了成本和复杂性。目前尚不清楚这种方法是否会在 ARIN 即将在 2020 年末发布的 IRR 和 RPKI 更新中保留。ARIN 在私人通讯中指出：“目前，我们托管 RPKI 的用户界面颇具挑战性，这主要源于永远不会生成/请求/存储用于签署请求的 RPKI 方的私钥。我们的社区一再要求一

个非常简单的 ARIN 在线集成的 ROA 生成界面。如果不存储请求签名密钥，那么可能无法满足此易用性要求，因此选择保持不可抵赖性。”

6.2 其他 RIR 关于责任的观点

其他四个 RIR 似乎没有表达相同程度的担忧，或没有依赖隐式的使用协议。尤其是，RIPE-NCC 访问 RPKI 数据的条款和条件规定：“RIPE NCC 对任何直接或间接损失概不负责”[108]，但没有明确的免责声明。接受采访的一些专家表示，通过透明度和应用当前的工程最佳实践来减轻风险要比免责声明更好。

应当指出，在每个 RIR 社区中都在进行有关免责责任的讨论。如上文所述，依赖方可以是，也可以不是，任何特定 RIR 的成员。因此，目前没有供依赖方在全球范围内讨论这些责任问题的论坛。

7 使用 ROA 覆盖通向关键基础设施的路径

ARIN 的依赖方协议说明[109]：

> *“您承认并同意，[在线资源证书 PKI]服务(或其任何部分)或证书不是为了危险环境下的设备或需要故障安全性能的用途而设计、认定或授权的，这些设备或用途包括与核设施、飞机导航或通信系统、空中交通管制系统或武器控制系统的操作有关的使用，和发生故障可能会导致死亡、人身伤害或严重的环境破坏的情况。”*

除了这些明确的限制外，人们可能想知道是否应该使用 RPKI 覆盖通往关键互联网基础设施的路径。在 ICANN 世界中，这个问题是：ROA 是否应覆盖 DNS 根服务器的前缀？同样，ROA 是否应覆盖 DNS 顶级域(TLD)权威服务器的前缀？

第一个观察结果是有十三台根服务器。如果一个被 BGP 路由泄漏破坏，则合理的假设是其他十二个将承担额外的负载。在最近的事件中可以看到，根服务器事故可能会发生，并且发生事故时管理覆盖这些服务器 IP 地址前缀的 BGP 通告是一个重要问题[110]。但是，目前尚不清楚 RPKI 起源验证的领域是否可以起到很多帮助。这种观察结果在一定程度上也适用于 TLD 权威服务器。

108 https://www.ripe.net/manage-ips-and-asns/resource-management/certification/legal/ripe-ncc-certification-repository-terms-and-conditions
109 https://www.arin.net/resources/manage/rpki/rpa.pdf
110 https://www.isc.org/docs/f-root/incident-2020-01.pdf

第二个观察结果是关于十三台 DNS 根服务器使用的地址的起源。这些前缀中的九个由 ARIN 分配，两个来自 RIPE NCC，一个来自 APNIC。ARIN 发生灾难性故障(例如 5.5 节中描述的故障)将产生不成比例的后果。一个可能的缓解方法是，某些根服务器操作员将其前缀转移到其他 RIR 来重新平衡风险。

第三个观察结果是，特别对于 DNS，已经存在一种保护系统安全的机制：DNSSEC。DNSSEC 基于数据完整性，而不是传输完整性。使用哪个根服务器实例无关紧要；重要的是根 DNS 数据是否经过验证。然后，目前的重点是通过在不同级别上组合不同的安全性机制产生的额外的安全性与额外的复杂性之间权衡。鉴于 RPKI 起源验证只能防止简单的路由系统攻击，因此成本效益的权衡尚不明确。

仅从这三个观察结果来看，很难用 ROA 为通往 DNS 根服务器的路径提供保护。

概括讨论以签署(或不签署)关键基础设施的 ROA(而不只是 DNS 根服务器的)，必须牢记第 4 章中描述的不同 RPKI 风险。由于某些 Tier 1 ISP 已在执行 ROV，因此关键基础设施运营商将必须都准备好应对 RPKI 根上任何违反安全性的后果，无论运营商自己是否决定签署 ROA。

因为从第 5 章分析中可以看出，如果在与起源地址块的 RIR 不同的 RIR 发生违规行为的情况下，使用 ROA 发布前缀的做法比不使用 ROA 的做法安全性要好一些，因此为根服务器签署 ROA 对安全性可以起到积极作用。

8 结论

在 RIR 们和大型与小型的网络运营商推动下，RPKI 引起了人们极大的兴趣。许多人士认为，RPKI 有足够容易实现的目标，可以带来正面的投资回报。现在，签署 ROA 变得非常简单，几乎所有 IP 地址所有者都可以做到这一点，并且 RPKI 起源验证提供了防止“胖手指”错误、配置错误和软件错误的保护机制。尽管 RPKI 起源验证不能防止对路由系统的复杂攻击，但从操作员的角度来看，对路由系统的攻击和由“胖手指”造成的路由泄漏都会产生必须处理的故障单。在这方面，RPKI 起源验证提供的任何帮助将肯定会受到许多 ISP 的欢迎。

但是，基于 X.509 证书的整个系统很复杂。这种复杂性带来了新的风险，新的错误、打字错误和“胖手指”仍会出现在 RPKI 自身之中。对于密码系统管理具备强大的专业知识可能仍将是开启 ROV 的前提条件。RPKI 本身并非没有问题。可能长达 24 小时的传播延迟，再加上缺乏广泛的系统监控，可能是一个主要的运营问题。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 起源验证还可能给路由系统带来新的威胁，例如对 RPKI 资料库、各种

证书或 ROA 分布式系统进行攻击的情况。迄今为止，RPKI 起源验证 ROV 仅在有限的范围内部署。RPKI 仍然存在与整个系统的可扩展性有关的未解决问题。

最终，由 RPKI 起源验证的相当精细的基础架构和操作复杂性所带来的开销，是否值得在路由完整性方面获得收益的价值，这是网络运营商需要做出的一个决定。一些网络运营商担心错误配置引起的路由泄漏对其运营造成影响，显然认为不值得采用 RPKI，而其他对路由安全性表示担忧的网络运营商对此也尚未确信。也许更重要的是，RPKI 确实意味着对整个互联网的关键运营结构进行了某些更改。尚不清楚参与这些变化并受其影响的社区是否充分意识到这些影响。对 RPKI 的影响进行交流的进一步工作明显是必要的。

9 致谢

尽管报告中的所有观点均为作者的观点，但我们想感谢以下人员在本报告的撰写过程中提供了意见、反馈或评论：

- 阿兰·艾伊纳（Alain Aina），中西部非洲研究和教育网络（West and Central African Research and Education Network，WACREN）
- 罗伯·奥斯汀（Rob Austein），Hactrn
- 约翰·柯伦（John Curran），美洲互联网号码注册管理机构（ARIN）
- 金·戴维斯（Kim Davies），互联网名称与数字地址分配机构 ICANN（互联网数字分配机构 IANA）
- 杰夫·休斯顿（Geoff Huston），亚太网络信息中心（APNIC）
- 弗雷德里克·科斯贝克（Fredrik Korsback），亚马逊公司（Amazon）
- 娜塔莉·昆纳克·特雷纳曼（Nathalie Künnake-Trenaman），欧洲 IP 网络资源协调中心（RIPE NCC）
- 马丁·利维（Martin Levy），Cloudflare
- 马迪，互联网域名系统北京市工程研究中心（ZDNS）
- 特里·曼德森（Terry Manderson），ICANN（DNS 和网络工程）
- 卡洛斯·马丁内斯（Carlos Martinez），拉丁美洲和加勒比地区的互联网地址注册处（LACNIC）
- 克里斯托弗·莫罗（Christopher Morrow），Google
- 里卡多·帕塔拉（Ricardo Patara），巴西网络信息中心（NIC Brazil）
- 阿姆雷什·福克（Amreesh Phokeer），非洲网络信息中心（AFRINIC）
- 安德烈·罗巴切夫斯基（Andrei Robachevsky），国际互联网协会（ISOC）
- 乔布·斯尼德斯（Job Snijders）, NTT
- 比尔·伍德科克（Bill Woodcock）, PCH（Packet Clearing House）

特别感谢 ICANN 的 David Huberman 在撰写本文时一直的支持和作为一名咨询者的意愿。