



基于本地信任锚点管理的 RPKI 安全运行机制研究

马 迪^{1,2}, 沈 烁³

(1. 互联网域名系统北京市工程研究中心 北京 100190;

2. 北龙中网(北京)科技有限公司 北京 100190; 3. 中国互联网络信息中心 北京 100190)

摘 要: 基于互联网当前的码号资源(IPv4 地址、IPv6 地址和 AS 号)分配体系, RPKI 的部署旨在提供一个认证互联网码号资源授权关系的平台, 以构建一个安全的域间路由系统。RPKI 的出现将域间路由系统安全由技术范畴迁移至运行管理范畴。为了应对 RPKI 的运行管理风险, 一种称为 RPKI 本地信任锚点的技术应运而生。对基于本地信任锚点的 RPKI 安全运行机制进行了介绍, 分析了该技术的不足, 并梳理了 RPKI 安全运行机制范畴今后可能的研究方向。

关键词: 互联网码号资源管理; 域间路由安全; 网络管理; 网络运行

doi: 10.3969/j.issn.1000-0801.2013.09.010

Study on RPKI Safeguard Based on Local Trust Anchor Management

Ma Di^{1,2}, Shen Shuo³

(1. Internet Domain Name System Beijing Engineering Research Centre, Beijing 100190, China;

2. KNET Technologies Co., Ltd., Beijing 100190, China; 3. China Internet Network Information Centre, Beijing 100190, China)

Abstract: RPKI is a PKI designed to support validation of claims by current holders of internet number resources (IPv4 addresses, IPv6 addresses and AS numbers), which is employed to establish a secure inter-domain routing system. However, the deployment of RPKI has its own risks falling into the category of operations and management. To give countermeasures, local trust anchor management for RPKI was introduced to build RPKI safeguard. A brief introduction to RPKI safeguard based on local trust anchor management was given, its shortcomings were analyzed and hence the potential research points of RPKI safeguard for the coming future were presented.

Key words: internet number resources management, security of inter-domain routing, network management, network operation

1 引言

1.1 RPKI

RPKI(resource public key infrastructure,资源公钥证书体系)^[1]是一个用于保障互联网码号资源(IP地址、AS号)分配关系真实性的认证系统,其基础技术的标准化工作已在IETF的SIDR(security of inter-domain routing,域间路由安全)工作组完成。继DNSSEC之后,RPKI成为ICANN

(the Internet Corporation for Assigned Name and Number)下一个重点推广和部署的互联网基础设施。伴随着APNIC(亚太互联网信息中心)、RIPE NCC(欧洲互联网信息中心)等全球五大地址注册机构(regional internet registry, RIR)开始提供基于RPKI的资源认证服务,RPKI及其衍生的资源认证服务将对互联网的运行产生重大影响^[2]。

RPKI技术体系的研发与部署源自一种众所周知的互联网安全威胁——路由劫持。由于BGP缺乏对路由通告



内容真实性的保证,黑客的蓄意攻击以及错误的网络参数配置都可以导致路由劫持现象的发生。见诸报端的典型路由劫持事件有:1997年4月的“AS 7007 Incident”、2004年12月土耳其 TTNNet 路由劫持事件、2006年1月 Con-Edison 路由劫持事件以及 2008年巴基斯坦电信劫持 YouTube 流量事件等。为增强域间路由系统的安全,不少研究工作面向 BGP 层面的缺陷给出了对策。其中,由美国 BBN 公司 Kent S 博士设计的 S-BGP^[3]提出了 RPKI 的概念及原型。

RPKI 是一种公钥证书基础设施。根据当前的全球互联网码号资源分配关系,RPKI 构建了一个面向 IP 地址及 AS 号码的授权认证体系,并以 X.509 证书扩展^[4]及若干签名对象的形式加以呈现。在 RPKI 中,码号资源的分配者在分配资源的同时,为其分配下游节点签发资源证书(基于 X.509 证书的扩展)。依托 RPKI 提供的认证功能,IP 地址的最终用户单位(资源持有者)通过发布一种称为路由起源声明(route origin attestation, ROA)的签名对象^[5,6],将特定的 IP 地址前缀授权给某个 AS 进行路由广播。作为 RPKI 认证体系的依赖方(relying party, RP),参与域间路由交互的网络运行单位(运营商、大型企业网络等)定期从 RPKI 资料库系统^[7](基于码号资源分配关系组织起来的分布式数据存储体系)同步资源证书以及包括 ROA 在内的签名对象集合,并将经过验证的信息(IP 地址前缀和 AS 号的映射关系)推送给边界路由器,供其在接收路由通告时进行真伪判断。

1.2 RPKI 运行风险

通过将“互联网码号资源”扩展项引入 X.509 证书,RPKI 在公钥证书体系中实现了互联网码号资源授权关系的认证。证书路径的构建是实施相关认证的关键,而信任锚点的选择则是证书路径构建的基础。RPKI 的认证关系由互联网码号资源的分配关系决定,APNIC、RIPE NCC 等互联网注册机构通过签发证书作为 RPKI 的一般“信任锚点”对 RPKI 体系施加管理和控制。因此,RPKI 的本质是在互联网码号资源范畴构建了一个基于“权威认证”的自上而下的层次化管理体系,放大了 ICANN 以及 APNIC 等 RIR 机构在互联网范畴的权力和影响力。这种影响力可能为互联网的运行安全带来新的风险。一旦 RIR 的 RPKI 组件出现问题,其负面影响将直接进入互联网的域间路由系统。例如,某个 RIR 如果错误地将其会员 ISP 的 IP 地址证书撤销,该运营商的 IP 地址空间将在 RPKI 空间中无效,可能进而导致该 ISP 网络在互联网上出现“路由不可达”

的危险局面。换言之,RPKI 将域间路由系统的安全问题由技术范畴迁移至了运行管理范畴。

2 本地信任锚点管理技术

RPKI 运行风险来自互联网码号资源管理权限的集中化。基于这一认知,美国 BBN 公司的技术团队在 RPKI 范畴引入了“本地信任锚点(local trust anchor, LTA)”的概念,设计了一种称为“RPKI 本地信任锚点管理”的安全技术^[8]。RPKI 本地信任锚点管理在本地重新构建一个证书体系,用以覆盖从外部 RPKI 资料库系统获得的“资源分配关系”,从而避免 RPKI 体系错误配置导致的本地网络运行故障。小至一个运营商网络,大至一个国家或者地区,都可以使用“RPKI 本地信任锚点”来保护其码号资源在其管理范围内的正确使用。

考虑到 RPKI 本地信任锚点管理技术在 IETF 的标准化工作正在进行,本节仅对其整体思路进行介绍。

2.1 RPKI 本地信任锚点管理的信任来源

RPKI 本地信任锚点管理的核心思想是,以 RPKI 依赖方为锚点在本地重新构建一个码号资源认证体系,该体系所反映的资源分配关系来自一个称为“约束文件(constraints file)”的外部信任源。根据“约束文件”提供的互联网码号资源授权情况,RPKI 依赖方以自身为“信任锚点”在本地重新签发相关证书来完成认证体系的重构。

“约束文件”是一个结构化的文档,提供了 RPKI 依赖方在本地构建互联网码号资源授权认证体系所需的必要信息,包括本地信任锚点密钥信息、证书处理策略以及码号资源列表。其中,码号资源列表是“约束文件”的必要构成,给出了 RPKI 资源证书与互联网码号资源绑定关系的集合。参考文献[8]对“约束文件”的主要内容及语义进行了说明,其最关键的部分是给出待修改资源证书(目标资源证书)的 SKI(证书主体公钥标识符)及其绑定资源的列表,如图 1 所示。如果“约束文件”反映的授权关系和 RPKI 资料库系统所提供的内容冲突,RPKI 依赖方以“约束文件”的内容为准。

“约束文件”的内容由其提供者决定,以带外方式导入 RPKI 依赖方的“本地”。“约束文件”的作用类似于抽象模型,RPKI 依赖方实现的本地信任锚点是该抽象模型的具象实例。导入了同一个“约束文件”的 RPKI 依赖方会生成一致的本地信任锚点。

```

SKI 0011223344556677889998877665544332211
IPv4
10.2.3/24
10.8/16
IPv6
2001:db8::/32
AS#
60123
5507

```

图1 “约束文件”码号资源列表条目参考示例

图2给出了“约束文件”和RPKI本地信任锚点的关系。

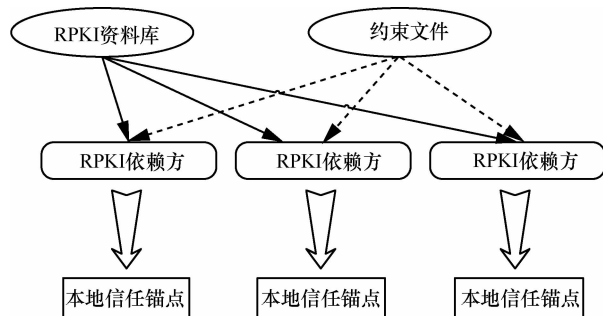


图2 “约束文件”与RPKI本地信任锚点的关系

2.2 RPKI资源证书的本地化处理

在导入外部信任源提供的“约束文件”后,RPKI依赖方对已经从RPKI资料库系统同步到本地的资源证书进行处理。根据“约束文件”中给出的SKI列表,RPKI依赖方确定待处理的“目标资源证书”。RPKI资源证书本地化处理的首要步骤是RPKI依赖方根据“约束文件”提供的“知识”重构码号资源的授权认证关系。也即,对于目标资源证书所绑定的码号资源,RPKI依赖方作为信任锚点绕过该资源证书的CA(上游一级或多级),直接签发证书进行认证。

假定经由互联网五大地址注册机构分配的码号资源集合分别表示为AF(非洲)、AP(亚太)、RN(欧洲)、LC(拉美及加勒比)及AR(北美),其中,经由APNIC分配出去的码号资源集合SS、KK以及经由RIPE NCC分配出去的码号资源集合ZZ的资源证书SKI,出现在某个RPKI依赖方信任的“约束文件”中,那么RPKI依赖方将签发新的资源证书以直接认证SS、KK及ZZ 3个码号资源空间的授权关系。同时,RPKI依赖方还需在本地对APNIC的自签名资源证书(包含了SS、KK两个码号资源集合)和RIPE NCC自签名资源证书(包含了码号资源空间ZZ)重新签发。由于

SS、KK及ZZ的授权关系将被RPKI依赖方(本地信任锚点)直接认证,为了避免冲突,需从APNIC的自签名资源证书和RIPE NCC自签名资源证书中将其移除,即“证书打孔(perforation)”。经过“证书打孔”,在RPKI依赖方维护的RPKI签名对象本地缓存中,APNIC资源证书所绑定的码号资源集合由AP减少为AP-SS-KK,RIPE NCC资源证书所绑定的码号资源集合由RN减少为RN-ZZ,形成了如图3所示的互联网码号资源授权认证关系。

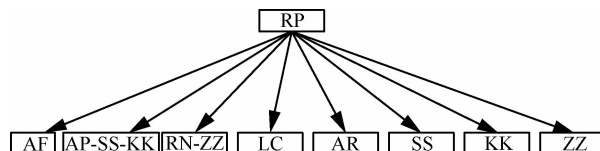


图3 RPKI资源证书的本地重签发示例

所谓证书重新签发,是指RPKI依赖方视自身为本地唯一的信任锚点,将相关资源证书“挂载”到自己的自签名资源证书之下。也即,RPKI依赖方对相关资源证书的原始信息进行修改并重新添加数字签名。对于不需要“打孔”的资源证书,RPKI依赖方在重新签发时,不改变其绑定的互联网码号资源。对于“约束文件”中未涉及的RPKI自签名资源证书,RPKI依赖方同样需要使用自己的私钥在本地对其重新签发,但新签发的证书主体保持不变,绑定资源也不变(如图3所示的码号资源集合AF、LC及AR)。

通过在本地“破坏”RPKI资源证书的完整性(重新签发),RPKI依赖方依据“约束文件”提供的信息,以自己为唯一的信任锚点在本地构建了一个RPKI认证体系“副本”。对“本地”的概念进行具象化处理,形成了“本地信任锚点”的具体应用场景。典型地,如果“本地”是指一个“国家或地区”,则该国家或地区范围内的RPKI依赖方通过导入一个权威实体发布“约束文件”,覆盖外部RPKI所反映的互联网码号资源授权关系。

3 本地信任锚点运行机制

参考文献[8]仅对RPKI本地信任锚点的基本原理和技术细节进行了说明,没有在运行层面给出RPKI本地信任锚点的操作方法,RPKI运行风险问题没有得到完全解决。然而,RPKI本地信任锚点管理技术的出现开启了RPKI安全保障体系的研究方向。根据RPKI本地信任锚点管理的基本原理,本节对本地信任锚点管理运行机制的相关问题进行阐述和分析,包括“约束文件”的管理和本地信任锚点管理的扩展应用。



3.1 “约束文件”管理

“约束文件”管理是 RPKI 本地信任锚点运行体系中最关键的要素,其选择和使用需谨慎为之。一旦“约束文件”中出现了错误的互联网码号资源授权信息,所有导入了该“约束文件”的 RPKI 依赖方则全在受影响之列,而这些 RPKI 依赖方所服务的 BGP 路由器在进行路由决策时也将受到不利影响。因此,“约束文件”的来源必须足够可信,导入机制必须足够安全。根据“约束文件”的基本功能,本节对其管理机制进行分析研究。

(1)“约束文件”的生成

尽管“约束文件”的呈现形式尚存在变化的可能,但是其基本内容已经在参考文献[8]中明确,也即资源证书的 SKI 同相关码号资源的绑定关系。这些绑定关系由“约束文件”提供方对外发布,其内容获得方法的备选方法可概括为两种模式:主动模式和被动模式。在主动模式下,“约束文件”提供方根据 RPKI 资料库的信息以及自己掌握的互联网码号资源授权知识,自主产生“约束文件”的相关条目,发布 SKI 与码号资源的绑定关系,供需要部署 RPKI 本地信任锚点的 RPKI 依赖方下载使用;在被动模式下,互联网码号资源的持有者(RPKI 资源证书持有者)向“约束文件”的提供方“备案”自己资源证书信息(SKI 及其绑定的码号资源),待“约束文件”提供方验证后写入“约束文件”并发布。

“约束文件”内容生成的两种模式适用于不同的 RPKI 本地信任锚点应用场景和不同的码号资源分配格局,需要统筹考虑运营商、互联网码号资源持有者以及“约束文件”提供者之间在实际业务中的关系。一般来说,如果担心资源证书被错误或者恶意地撤销,RPKI 资源证书持有者可以选择采用被动模式,向一个能够被运营商信任的第三方实体备案其持有的资源证书信息;而如果一个国家或地区有意识地想借助 RPKI 本地信任锚点保护其管辖范围的互联网码号资源,可以选择采用主动模式,将该国家或地区范围内的资源授权情况通过“约束文件”发布出去。因此,面向具体网络场景的本地信任锚点部署机制是 RPKI 在我国落地需要研究的问题。

(2)“约束文件”的分发

对于 RPKI 本地信任锚点的核心,参考文献[8]并未对“约束文件”的分发机制提供参考,但该问题在实践层面无法回避。一方面,由于互联网不是一个天然的安全通信环境,“约束文件”的分发机制依赖安全保障技术,相关对策

或将数字签名引入“约束文件”,或设计借助提供数据完整性的安全通信协议;另一方面,互联网码号资源授权关系的变化会导致“约束文件”的更新,需及时地向 RPKI 依赖方反馈,“约束文件”的分发机制还应提供数据同步功能。因此,“约束文件”的分发机制需要考虑 RPKI 依赖方和“约束文件”提供者之间的关系、RPKI 依赖方分布范围以及“约束文件”的更新频率等因素。设计一个兼顾安全性和时效性的“约束文件”分发机制将是 RPKI 本地信任锚点管理技术的运行关键。

根据 RPKI 本地信任锚点管理的当前设计版本^[9],一个 RPKI 依赖方只能导入一个“约束文件”。但在实践中,一个运营商可能倾向同时导入来自多个信任源且彼此之间没有冲突的“约束文件”,以保护其网络下游客户的码号资源,因此相关的技术标准化在 IETF 的进展值得持续关注。

3.2 本地信任锚点的扩展应用

基于 RPKI 本地信任锚点管理的 RPKI 安全运行机制,仅在“本地有效”,也即在选择同一“约束文件”的 RPKI 依赖方之间发挥作用。导入同一“约束文件”的 RPKI 依赖方越多,该“约束文件”所保护的範圍越广。可见,基于本地信任锚点管理的 RPKI 安全运行机制的作用范围,取决于“约束文件”在多大范围内被不同的 RPKI 依赖方所信任。换言之,在“约束文件”不被信任的范围,“约束文件”中列出的码号资源无法被该范围内的 RPKI 本地信任锚点施加保护。例如,一个运营商的 IP 地址资源证书如果被地址注册机构撤销,那么该地址空间在 RPKI 系统中呈现“不可用”的状态;基于 RPKI 本地信任锚点管理,如果该地址空间的授权关系经由“约束文件”被发布出去,这种“不可用”状态可以在某个局部范围被修复,但没有导入该“约束文件”的 RPKI 依赖方(其他运营商)仍然可能视该 IP 地址空间无效。

本地信任锚点的部署可以避免外部的 RPKI 错误配置影响到“本地”内部的域间路由,但无法将正确的码号资源授权关系传播到本地以外的域间路由系统。从互联互通的意义出发,本地信任锚点的基本应用无法完全支撑起 RPKI 安全运行体系。在未来的 RPKI 安全保障体系研究范畴,相关的对策应从“约束文件”的“广播机制”角度出发,使得码号资源持有者能够自主地发布相关绑定关系,并被 RPKI 依赖方察觉、下载以及参考。一种可能的思路是,在不同范围具有权威的“约束文件”提供者可以通过带外信任关系,互相交换、共享码号资源的授权关系,形成类似于信任联盟的组织来平衡 APNIC 等地址注册机构可能会对

域间路由系统产生的控制力。

4 结束语

RPKI 在全球范围的部署为构建一个安全的互联网域间路由系统,奠定了一个可信的基础设施。但是,RPKI 的部署使得原来扁平化的域间路由体系运行模式,受到了来自层次化认证体系的管理,形成了一个以 ICANN 为根(或 APNIC 等五大地址注册机构)的互联网码号资源的授权认证树。RPKI 认证树的出现,带来了新的运行管理风险。针对互联网码号资源证书的错误或者恶意撤销行为,或将成为域间路由安全的新隐患。尽管这一隐患不是 RPKI 技术体系的内在缺陷,但互联网社区必须在 RPKI 运行实践层面审慎考虑并妥善处理。

RPKI 作为面向全球范围的互联网安全基础设施,同时影响互联网码号资源的分配管理和域间路由系统的运行,因此 RPKI 的安全运行机制应当作为我国互联网安全保障体系新的必要组成部分。我国的运营商和内容提供商正经历由 IPv4 到 IPv6 的过渡,且存在复杂的 IP 地址资源分配格局。为了在利用 RPKI 保护域间路由安全的同时,消除 RPKI 的不利因素,骨干网运营商、地址注册机构以及持有较多地址资源的组织机构需相互配合,积极开展 RPKI 本地信任锚点在我国的应用模式研究。

参考文献

- 1 马迪. RPKI 概览. 电信网技术, 2012(9)
- 2 马迪. 互联网资源认证业务发展状况. 2012-2013 中国通信业

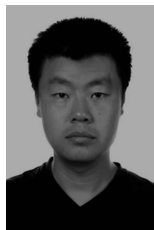
发展分析报告, 2013

- 3 Kent S, Lynn C, Seo K. Secure border gateway protocol (S-BGP). IEEE Journal on Selected Areas in Communications, 2000(4)
- 4 Lynn C, Kent S, Seo K. X.509 Extensions for IP Addresses and AS Identifiers. RFC3779, 2004
- 5 Lepinski M, Kent S, Kong D. A Profile for Route Origin Authorizations (ROAs). RFC6482, 2012
- 6 Huston G, Michaelson G. Validation of Route Origination Using the RPKI and Route Origin Authorizations. RFC6483, 2012
- 7 Huston G, Loomans R, Michaelson G. A Profile for Resource Certificate Repository Structure. RFC6481, 2012
- 8 Local Trust Anchor Management for the Resource Public Key Infrastructure. draft-ietf-sidr-ltamgmt-08, 2013

[作者简介]



马迪,男,博士,现就职于互联网域名系统北京市工程研究中心,主要研究方向为下一代互联网、互联网资源寻址定位。



沈烁,男,博士,中国互联网络信息中心副研究员,主要研究方向为计算机网络、信息安全。

(收稿日期:2013-06-05)

· 简讯 ·

2013 年 7 月份通信业经济运行情况

2013 年 7 月我国通信业总体保持平稳运行。

电信主营业务收入月规模突破 1 000 亿元。7 月份,全国电信业务总量完成 1 175.2 亿元,同比增长 8.3%;电信主营业务收入完成 1 002.7 亿元,自 2011 年以来首次突破 1 000 亿元,同比增长 7.8%。1-7 月,全国电信业务总量累计完成 8 045.4 亿元,同比增长 7.9%,与上半年增速持平;电信主营业务收入累计完成 6 645.3 亿元,同比增长 8.8%,比上半年小幅回落 0.1 个百分点。

3G 新增用户突破 1 亿户,用户渗透率达到 28.2%。1-7 月,全国移动电话用户净增 7 307.4 万户,总数达到 11.85 亿户。其中,3G 移动电话用户净增 10 093.5 万户,相当于 2012 年全年净增总数,3G 用户总数达到 3.34 亿户,在移动用户中占比 28.2%,预计第 3 季度末将突破 30%。受 TD 终端加速推广和数据业务需求提高的刺激,TD 电话占比明显提高。1-7 月累计 TD 用户净增 5 875.4 万户,总数达到 1.47 亿户,占中国移动的移动电话用户比重由 2012 年末的 12.1% 提升至 19.3%。

(来源:工业和信息化部运行监测协调局)