

互联网名址体系安全保障技术及其应用分析

王翠翠^{1,2}, 延志伟^{1,2}, 耿光刚^{1,2}

(1. 中国互联网络信息中心, 北京 100190;

2. 互联网域名管理技术国家工程实验室, 北京 100190)

摘要: 为了确保域名系统与域间路由系统的安全运行, 互联网工程任务组(IETF, internet engineering task force)提出了2项互联网名址体系安全保障技术——DNS安全扩展(DNSSEC, domain name system security extention)与资源公钥基础设施(RPKI, resource public key infrastructure)。在域名系统层面, DNSSEC通过使用公钥基础设施在DNS原有的体系结构上添加数字签名, 为DNS提供了权限认证和信息完整性验证, 成为了域名系统安全的基石; 域间路由系统层面, RPKI通过公钥证书对互联网码号资源的所有权和使用权进行认证, 构建了一个支撑域间路由安全的互联网基础资源管理体系。近年来, DNSSEC与RPKI在全球范围内的部署不断推进, 为了解其在全球互联网的应用情况, 以Alex前10⁶个网站为数据集, 对2项互联网名址体系安全保障技术及其应用状况进行了研究与分析。

关键词: 域名系统; 域间路由系统; DNS安全扩展; 资源公钥基础设施

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00147

Internet naming and addressing system security technology and application analysis

WANG Cui-cui^{1,2}, YAN Zhi-wei^{1,2}, GENG Guang-gang^{1,2}

(1. China Internet Network Information Center, Beijing 100190, China;

2. National Engineering Laboratory for Internet Domain Name Management, Beijing 100190, China)

Abstract: In order to ensure the security of domain name system and inter-domain routing system, Internet Engineering Task Force (IETF) proposed two kinds of security technology, namely domain name system security extension (DNSSEC) and resource public key infrastructure (RPKI). For the domain name system, DNSSEC added the digital signature to the original architecture of DNS using the public key infrastructure and it provided the authentication and integrity verification of DNS information, which became the anchor of domain name system security. For the inter-domain routing system, RPKI utilized the public key certificate to authenticate the ownership and usage rights of the Internet number resources and builds an Internet resource management system to enhance inter-domain routing security. Recently, the globally development of DNSSEC and RPKI were continuously expanding. In order to research the application of the two kinds of technology, Alexa top 1 million websites were taken as the data set to study and analyze the application status of DNSSEC and RPKI.

Key words: domain name system, inter-domain routing system, domain name system security extension, resource public key infrastructure

收稿日期: 2017-01-05; 修回日期: 2017-02-16. 通信作者: 王翠翠, wangcuicui@cnnic.cn

基金项目: 国家自然科学基金资助项目 (No.61375039, No.61303242)

Foundation Item: The National Natural Science Foundation of China (No.61375039, No.61303242)

1 引言

随着互联网的飞速发展及网络安全事件的频发,互联网安全成为业界热切关注的议题。域名系统和域间路由系统承担着保障互联网互联互通的重要职能,因此其平稳运行对互联网的安全至关重要。

作为互联网重要的基础设施之一,域名系统(DNS, domain name system)是一种分布式的等级制查询服务,用以在域名和IP地址间进行翻译转换,是网民访问网络应用的唯一入口。

但作为互联网中的早期协议,DNS体系结构建立在互信模型之上,缺乏DNS信息的完整性保障和认证机制。因此,攻击者可发动中间人攻击注入错误的响应信息,并在检验其合法的情况下被查询者接收,该类攻击被称作DNS欺骗攻击(DNS spoofing)。在DNS运行机制中,为了避免对同一查询重复发送请求,在接收到DNS权威服务器返回的查询结果后,递归服务器会将结果进行保存,并设置一定的保存时长,这样就形成了DNS缓存。基于该机制DNS欺骗攻击的响应信息会通过污染DNS缓存构成DNS缓存投毒攻击,导致后续针对该记录的查询均返回伪造的响应信息。

DNS系统的脆弱性以及其对互联网的至关重要性,使其极易成为黑客的攻击目标。近年来,DNS安全攻击事件频繁见诸报端:2010年1月,百度遭遇DNS劫持;2011年9月,微软、宏碁等众多知名网站遭遇DNS劫持;2014年1月,全国DNS故障;2015年11月,DNS根服务器遭遇攻击;2015年12月,土耳其国家顶级域遭攻击。随着DNS攻击事件频繁发生,DNS的安全性日益突出。

作为域间路由系统层面的关键基础设施,边界网关协议(BGP, border gateway protocol)通过交换互联网中自治域系统(AS, autonomous systems)之间的路由宣告,实现自治域系统间的互联互通。然而BGP在设计方面的设计存在严重不足:BGP默认接受AS通告的任何路由,因此即使一个AS向外通告不属于自己的IP前缀,该通告也会被对端接受并继续传播。正是因为

BGP在设计方面的这一安全缺陷,使网络中恶意用户的蓄意攻击以及网络管理员错误的参数配置都可能导致一种严重的互联网安全威胁——路由劫持。

近些年,发生的典型路由劫持包括:2004年12月的土耳其电信集团劫持互联网事件^[1];2008年2月的巴基斯坦劫持YouTube事件^[2];2014年2月的加拿大流量劫持事件^[3];2015年1月的美国ISP劫持日本地址前缀事件^[4];2015年11月的印度运营商Bharti Airtel劫持大量地址前缀事件^[5]等。路由劫持对互联网的正常运行影响非常大,可能会导致路由黑洞、流量窃听以及大规模的拒绝服务攻击^[6]等。

因此,互联网工程任务组(IETF, Internet Engineering Task Force)提出了2项互联网名址体系安全保障技术——DNS安全扩展(DNSSEC, domain name system security extention)与资源公钥基础设施(RPKI, resource public key infrastructure),用以保障域名系统及域间路由系统的安全运行。

2 互联网名址体系安全保障技术

2.1 DNSSEC

2.1.1 技术原理

为了保障DNS数据在传输过程中不被更改,IETF于1997年提出了DNSSEC技术体系。利用公钥基础设施(PKI, public key infrastructure),DNSSEC在DNS原有的体系结构上添加数字签名,为DNS消息提供了权限认证和信息完整性验证。

DNSSEC机制为DNS提供3方面的安全保障^[7]:1)为DNS体系提供数据来源验证,保障了DNS数据来源的准确性;2)验证数据完整性,确保数据在传输过程中不被篡改;3)为否定应答报文提供验证。

DNSSEC工作机制主要包括以下几步。

1) 基于公钥加密系统DNS服务器(一般是区内的主服务器)产生了一对密钥:公钥和私钥。

2) DNS服务器使用私钥对资源记录(RR, resource record)进行加密运算得到一个新的资源记录——RRSIG,并将RRSIG与RR作为应答报文发送给查询客户端。同时,RRSIG中还包含公

钥或数字签名算法的代码。

3) 针对接收到的应答报文, 客户端利用公钥和加密算法对其进行加密运算, 并将计算结果同应答报文中的 RRSIG 相比较, 如果二者相同, 则表明应答报文中的资源记录为真, 否则表明收到的资源记录被篡改。

在实际运行过程中, 每个 DNSSEC 区均有 2 个密钥对。第 1 个密钥对为区签名密钥(ZSK, zone signing key), 用于对 DNS 资源记录进行签名; 第 2 个密钥对为密钥签名密钥(KSK, key signing key), 用于对包含密钥(如 ZSK)的资源记录进行签名。

在 DNSSEC 体系中, 递归服务器首先用 KSK 公钥对 DNSKEY 进行验证, 然后用 ZSK 公钥对数据的完整性进行验证。如果递归服务器信任它所使用的 KSK 公钥, 则称该 KSK 公钥为该递归服务器的信任锚。

DNSSEC 区将其 KSK 公钥交给父区, 由父区用自己的私钥对其进行签名, 并以此类推, 这样的过程称为安全授权。利用安全授权的过程到达信任锚时, 形成了一条信任链。由于根区位于 DNS 层级结构中的最顶端, 且具有唯一性, 因此根区的 KSK 公钥成为所有区的信任锚。如果沿着信任链可到达根区, 那么通过使用根区的 KSK 公钥进行签名验证, 则可以保障数据来源的可靠性和数据本身的完整性。

2.1.2 部署现状

近年来, DNSSEC 在全球的部署逐步推进。

2010 年 7 月, ICANN 发布根区信任锚, 所有的根服务器完成了 DNSSEC 部署并正式宣布对外提供 DNSSEC 服务; 2011 年 3 月, 全球最大的顶级域.com 完成 DNSSEC 的部署; 2011 年 5 月 18 日, Nominet 在.uk 域内部署 DNSSEC; 2012 年 1 月, Comcast 宣布其所有的 DNS 解析器均支持 DNSSEC 验证, 且其服务范围内的所有区数据均已部署 DNSSEC; 截至 2012 年 4 月 6 日, 全球范围内完成 DNSSEC 部署的 TLD 已达 91 个, 占全部顶级域总数的 30.9%。

自 20 世纪末 DNSSEC 概念被提出以来, 其发展历程已达 20 年之久。作为保障互联网名址体系安全保障技术之一, DNSSEC 在全球主流网站

中的部署程度是决定全球互联网能否更加有序运作的因素, 但当前 DNSSEC 在全球的部署应用程度如何仍未可知。

2.2 RPKI

2.2.1 技术原理

为保障域间路由系统的安全, 一些针对 BGP 缺陷的解决方案相继被提出, 其中以 BBN 公司提出的 S-BGP (Secure BGP) 和思科公司提出的 soBGP (secure origin BGP) 在业界最具影响力。为了验证路由通告中 IP 地址前缀和传播路径上 AS 号之间的绑定关系, 防止路由劫持的发生, S-BGP 的方案中引入了一种附加签名的 BGP 扩展消息格式。将数字证书和签名机制引入了 BGP 范畴, 从而需要一套公钥基础设施的支持, RPKI 应运而生。

RPKI 通过构建一个公钥证书体系完成对互联网号码资源 (INR, Internet number resource) (包括 IP 前缀和 AS 号) 所有权 (分配关系) 和使用权 (路由源授权) 的认证, 所产生 “认证信息” 可进一步用于 BGP 路由器的路由决策, 帮助其验证 BGP 报文中路由源 AS 的真实性, 从而防止路由劫持的发生^[8]。RPKI 技术体系的基本功能之一是对 INR 的分配提供密码学上可验证的担保。当前互联网号码资源的分配为分层式架构: 最顶层是互联网号码分配机构 (IANA, Internet assigned numbers authority), IANA 将 INR 分配给 5 个区域性互联网注册机构 (RIR, regional Internet registry), 包括亚太互联网络信息中心、非洲互联网络信息中心、美国网络地址注册中心、拉丁美洲和加勒比地区互联网地址注册管理机构以及欧洲网络协调中心, RIR 将资源分配给其下级节点, 如本地互联网注册机构 (LIR, local Internet registry)、国家级互联网注册机构 (NIR, national Internet registry) 和互联网服务提供商 (ISP, Internet service provider), 下级节点再依照地址分配逻辑继续逐级向下分配资源。

为了保障 INR 的所有权和使用权, RPKI 体系中的任一节点在进行资源分配的同时, 将签发相应的证书。RPKI 体系主要包括 2 种证书: 认证权威 (CA, certificate authority) 证书^[9]和端实体 (EE, end entity) 证书^[10]。CA 证书用于保障 INR

所有权,EE证书则用于对路由源授权(ROA, route origin authorization)进行认证。RPKI路由起源认证中最重要的对象就是ROA,它为资源持有者授权某个AS,它为其所拥有的特定的IP前缀发起路由起源通告提供了担保。

如图1所示,RPKI的体系架构包括3个功能模块:CA、资料库(repository)和依赖方(RP, relying party)。这3个模块完成RPKI数字签名对象的签发、存储、验证,从而最终实现RPKI的路由起源认证功能。

1) 运行CA的实体机构包括IANA、RIR、NIR、ISP等。CA通过签发CA证书来证明INR的所有权,通过签发ROA授权某个AS针对特定的IP地址前缀发起路由起源通告。

2) 资料库用于存储CA发布的各种包含INR分配信息和授权信息的CA证书、ROA等数字签名对象,并提供给全球的依赖方进行同步和验证。

3) 依赖方从资料库中同步RPKI的数字签名对象,对这些数字签名对象进行验证后将其处理成IP前缀与AS号的合法授权关系,最后将该授权关系提供给BGP路由器,用于指导其路由决策。

最后,利用RPKI数据,开启RPKI的BGP路由器可对其接收的BGP更新消息进行验证。这样,BGP路由被分类为3种状态:valid、invalid

和unknown,进而可配置BGP路由器,通过拒绝一个不合法的路由宣告最终防止路由劫持的发生。

2.2.2 部署状况

近年来,RPKI在全球的部署逐步推进:2012年2月,IETF SIDR工作组发布了14个RPKI核心技术相关的RFC(RFC6480-RFC6493);2012年初,全球五大RIR已全部对其会员开放互联网资源认证业务^[11];2013年2月,JPNIC面向日本国内的运营商开放了公共RP服务^[12],并积极推动RPKI在日本的部署;2013年9月,南美洲厄瓜多尔国内的运营商在LACNIC的技术支持下,成功部署RPKI路由源认证系统^[13]。

同时,互联网工业界也在积极研究RPKI关键技术可能带来的新机遇:BBN公司开发了BBN Relying Party软件并进行相应的实验;Cisco、Juniper等厂商的路由设备也开始支持基于RPKI的路由起源验证,并推出了相应的产品;Alcatel Lucent也正积极研发支持RPKI的相关产品。

可见,RPKI技术体系对互联网应用的有序运行至关重要,但当前RPKI在全球互联网中的应用状况如何,仍处于未知状态。

因此,为了分析DNSSEC技术与RPKI技术在全球的应用状况,本文提出了针对2种技术应用状况的统计分析方法。

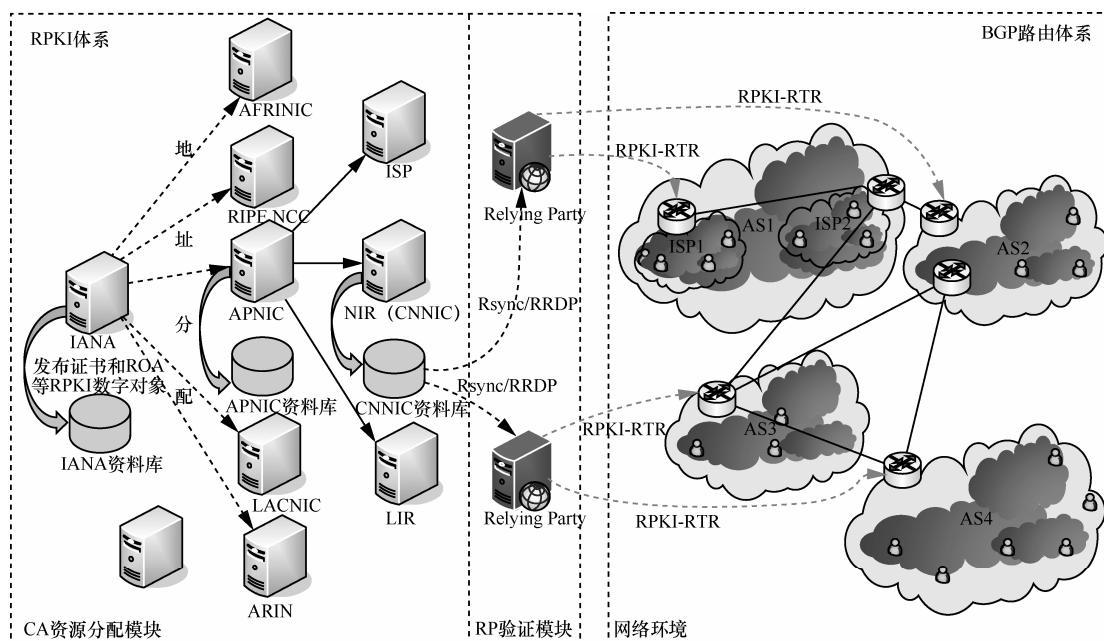


图1 RPKI体系架构

3 统计方法

在本文提出的统计方法中,考虑到网站是互联网应用最重要的构成部分,因此将 DNSSEC 与 RPKI 在全球主流网站中的应用率是其在互联网应用中应用程度的有效度量。所以,本文以 Alexa (专门发布网站世界排名的权威网站) 列表中前 10^6 的网站为数据集,分析 DNSSEC 与 RPKI 在全球主流网站中的应用率,用以分析 3 项互联网名址体系安全保障技术在全球的应用状况。

3.1 DNSSEC 应用状况统计方法

为了分析 Alexa 前 10^6 个网站中 DNSSEC 的应用状况,本文采用 Google DNS 公共递归服务器 (8.8.8.8) 对数据集中各网站对应的域名进行探测,并查看各个域名是否存在 RRSIG 记录。如存在,则提取各域名对应的 RRSIG 记录,并对 RRSIG 记录所使用的签名算法、TTL 等信息进行进一步分析。其中利用 Google 递归服务器进行域名探测的地点为北京,时间为 2016 年 3 月。

3.2 RPKI 应用状况统计方法

如图 2 所示,本文采用的 RPKI 应用状况统计方法中包括挑选网站样本、获取网站域名所对应的 IP 地址、获取 IP 地址对应前缀及源 AS、验证网站是否应用 RPKI 4 个步骤。

1) 挑选网站样本

本文采用了 Alexa 列表中前 10^6 个网站作为分析样本,这样也可以更清晰直观地了解 RPKI 在 Alexa 排名不同的网站中的应用状况。

2) 分析网站域名所对应的 IP 地址

为了分析 Alexa 前 10^6 个网站的域名所对应的 IP 地址,本文采用 Google DNS 公共递归服务器对各网站的域名进行探测,并提取各域名对应的 A 记录与 AAAA 记录。其中利用 Google 递归

服务器进行探测的地点为北京,时间为 2016 年 3 月。

3) 分析 IP 地址所对应的 IP 地址前缀以及宣告该前缀的 AS 号

本文采用了欧洲网络协调中心 (RIPE NCC, Reseaux IP Europeens Network Coordination Center) 所提供的接口用以获取 IP 地址所对应的 IP 地址前缀以及宣告该前缀的 AS 号 (即源 AS): <https://stat.ripe.net/data/network-info/data.<format>?<parameters>>。

该接口可根据给定的 IP 地址返回其对应的 IP 地址前缀及源 AS,其用法如下:如 <https://stat.ripe.net/data/network-info/data.json?resource=140.78.90.50>。

所需参数如表 1 所示。

表 1		所需参数	
参数选项	参数值	含义	是否必须
resource	IP 地址	想要获取的其 IP 地址前缀、源 AS 的 IP 地址及源 AS	是

返回值格式如表 2 所示。

表 2		返回值格式
选项		含义
asns		宣告 IP 地址前缀的 AS 号
prefix		指定的 IP 地址所在的 IP 地址前缀

返回值示例如下。

```
{
  "asns": [
    "5511",
    "6453"
  ],
  "prefix": "41.138.32.0/20"
}
```

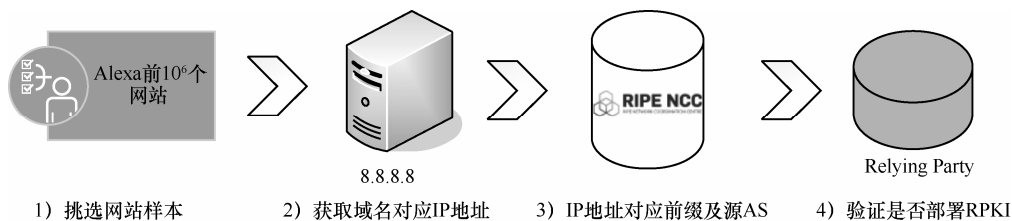


图 2 RPKI 覆盖状况统计方法

4) 验证网站是否部署 RPKI

本文采用 Dragon labs (<https://rpki.net>) 提供的 RPKI.net 软件包, 搭建完成 RP 节点, 并将 5 大 RIR 设为信任锚点, 获取各个信任锚点下的 ROA 签名对象并进行验证。

在 RPKI 体系中, BGP 路由合法性状态共为 3 种: valid、invalid 以及 unknown。在该步骤中, 以经验证后正确 ROA 数据为参照, 对步骤 3) 获取的 IP 地址前缀以及源 AS (也即路由) 的合法性进行判断。其中 RFC6483^[14]中定义了有关 BGP 路由合法性验证的方法。在已知路由的 IP 地址前缀及源 AS 的情况下, 其判定标准如表 3 所示。在本文所提出的统计方法中, 只有对应的网站 BGP 路由合法性状态为 valid, 才判定该网站已应用 RPKI。

表 3 BGP 路由合法性验证标准

路由前缀	AS 与 ROA 中匹配	AS 与 ROA 中不匹配
与 ROA 中前缀无交集	unknown	unknown
包含 ROA 中的前缀	unknown	unknown
与 ROA 中的前缀完全匹配	valid	invalid
比 ROA 中的前缀更具体	invalid	invalid

4 统计结果

4.1 DNSSEC 在 Alexa 前 10⁶ 个网站中的应用状况

4.1.1 应用率

经统计分析得出, Alexa 前 10⁶ 个网站中, 应用 DNSSEC 的网站数量为 15 869 个, 应用率约为 1.59%; 而在 Alexa 前 10⁵ 个网站中, 支持 DNSSEC 网站数量为 1 566 个, 支持率约为 1.57%

(如表 4 所示)。可见, 虽然 DNSSEC 的部署工作已历时 6 年, 但其在互联网中的应用率仍处于较低状态。

表 4 Alexa 前 10⁶ 个万网站 DNSSEC 部署率

网站	应用 DNSSEC 的网站数量/个	DNSSEC 应用率
Alex 前 10 ⁵ 个	1 566	1.57%
Alex 前 10 ⁶ 个	15 869	1.59%

4.1.2 应用地区分布

应用 DNSSEC 的网站分布于 80 多个国家和地区, 尤以美国应用程度最高, 如表 4 所示, 应用数量最多的前 4 位国家包括美国、荷兰、法国、捷克。

表 5 应用 DNSSEC 的网站数量最多的国家

网站所属国家	应用 DNSSEC 的网站数量/个
美国	3 878
荷兰	2 867
法国	2 170
捷克	1 570

4.1.3 TLD 分布

通过对支持 DNSSEC 的网站域名进行分析可见, DNSSEC 应用数量较多的前 5 位顶级域为: .com、.nl、.cz、.br 以及 .se, 其中各项级域中应用 DNSSEC 的网站数量分布如图 3 所示。

4.1.4 使用算法

对应用 DNSSEC 的网站进行进一步分析, 其在应用 DNSSEC 时所使用的算法代号分布如图 4 所示。

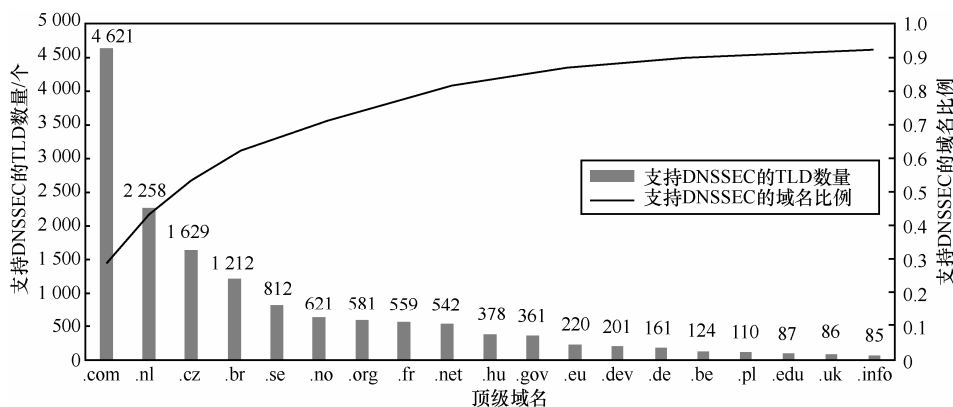


图 3 应用 DNSSEC 的顶级域分布

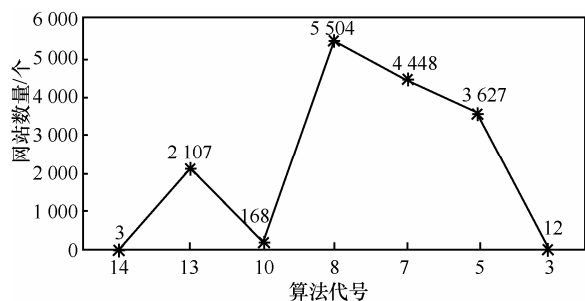


图4 应用 DNSSEC 的网站所使用的签名算法代号分布

进一步地,根据 IANA 有关 DNSSEC 算法代号的规定,图中所示的各算法代号其所代表签名算法如表 6 所示。

表 6 DNSSEC 签名算法代号及名称

算法代号	具体算法
14	ECDSAP384SHA384
13	ECDSAP256SHA256
10	RSASHA512
8	RSASHA256
7	RSASHA1-NSEC3-SHA1
5	RSASHA1
3	DSA

由图 4 及表 6 可见, DNSSEC 部署时使用最为普遍的算法为 RSASHA256、RSASHA1-NSEC3-SHA1、RSASHA1。

4.1.5 TTL 分布

对应用 DNSSEC 网站数量最多的前 10 位顶级域进行分析,由图 5 可见,平均 TTL 设置最高

的为.br, TTL 为 68 569.3 s, 设置最低的为.no, TTL 为 7 254.7 s。

4.2 RPKI 在 Alexa 前 10⁶ 个网站中的应用状况

4.2.1 应用率

经统计和分析, Alexa 前 10⁶ 个网站中, 应用 RPKI 的网站数量为 63 785 个, 应用率约为 6.4%。考虑到 RPKI 体系从提出到其逐步的部署仅只有不到 5 年的时间, 可见 RPKI 在全球的应用程度相较于 DNSSEC 已处于较高的水平。

表 7 Alexa 前 10⁶ 个网站 DNSSEC&RPKI 应用率对比

关键基础设施	应用 RPKI 的网站数量/个	应用率
DNSSEC	15 869	1.57%
RPKI	63 785	6.37%

4.2.2 应用地区分布

应用 RPKI 的网站遍布于世界 90 多个国家和地区。其中应用 RPKI 的网站在欧洲地区最为集中, 由此可见欧洲地区的 RPKI 部署发展最为迅速; 其次, 拉丁美洲地区的部分国家已开展了 RPKI 的部署工作; 对亚洲地区, 日本、马来西亚、印度、新加坡、菲律宾等数个国家已经开展了 RPKI 的部署; 同时数据分析显示, 美国有 112 例网站已经应用 RPKI, 相较于 DNSSEC 在美国的应用程度可知, 美国的 RPKI 部署工作尚处于初始阶段。

应用 RPKI 网站数量最多的前 10 位国家如表 8 所示, 其中德国居于首位。

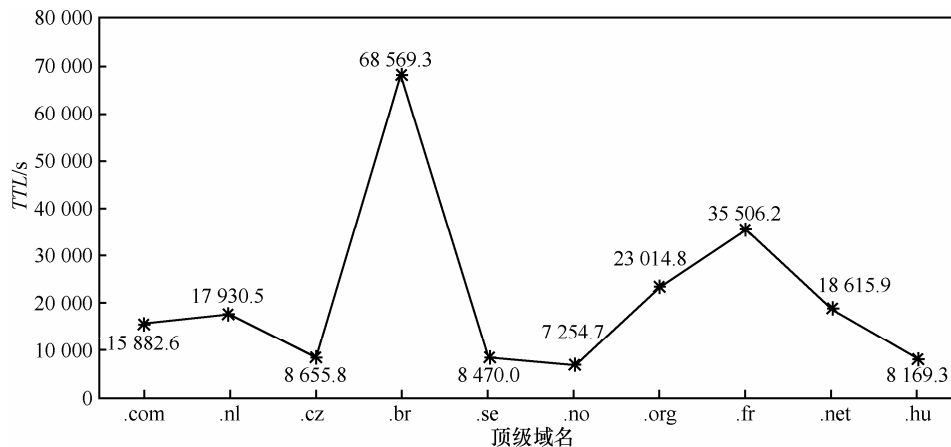


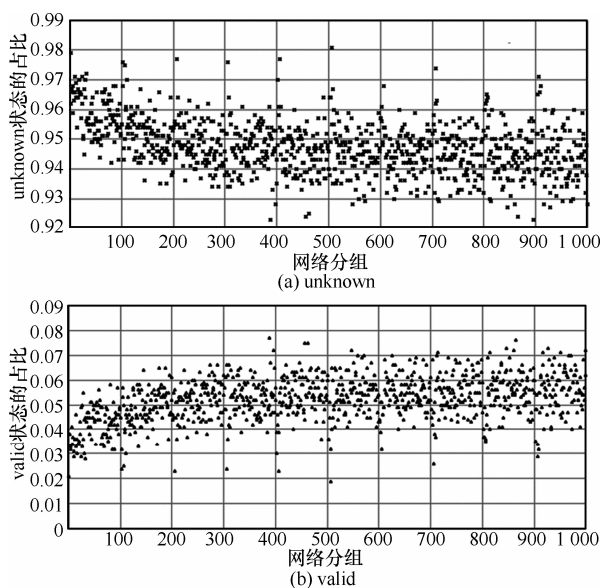
图5 前10位顶级域TTL分布

表8 应用 RPKI 的网站数量最多前 10 位国家

国家	应用 RPKI 的网站数量/个
德国	28 495
法国	7 397
俄罗斯	3 940
荷兰	3 330
英国	2 120
伊朗	1 912
捷克	1 379
土耳其	1 374
瑞典	1 223
瑞士	1 183

4.2.3 RPKI 体系下网站的 BGP 路由合法性状态分布

通过对 Alexa 前 10^6 个网站进行分组, 每 1 000 个网站为一组, 共获得 1 000 组数据。接下来, 对 RPKI valid\unknown\invalid 状态的网站数量进行统计。如图 6 所示, Alexa 前 10^6 个网站中 RPKI valid 的比例浮动范围为 $[0.015, 0.08]$, 且前 10^5 个网站的 RPKI 应用率明显低于后 10^5 个的网站。

图6 Alexa 前 10^6 个网站路由合法状态分布

经统计, RPKI invalid 状态的网站数量约为 174 个, 也就是说, 如果这些网站的 ROA 对象被运用到路由决策中, 极有可能造成这 174 个网站无法被用户访问。由此可见, 如何保障签发 ROA 的准确性也是决定 RPKI 体系能否全面部署及有

序运行的关键因素。

5 结束语

作为保证互联网互联互通基本特点的重要基础设施, 域名系统与域间路由系统的平稳运行是保障互联网安全的根本。为了确保域名系统及域间路由系统的安全运行, IETF 提出了 2 项互联网名址体系保障技术——DNSSEC 与 RPKI。在域名系统层面, DNSSEC 通过使用公钥基础设施在 DNS 原有的体系结构上添加数字签名, 为 DNS 提供了权限认证和信息完整性验证, 成为了域名系统安全的基石; 域间路由系统层面, RPKI 通过公钥证书对互联网码号资源的所有权和使用权进行认证, 构建了一个支撑域间路由安全的互联网基础资源管理体系。

近年来, DNSSEC 与 RPKI 在全球范围内的部署不断推进。为了解其在全球互联网的应用情况, 本文提出了针对 DNSSEC 与 RPKI 技术的应用状况分析方法, 通过以 Alexa 前 10^6 个网站为数据集, 分析 DNSSEC 与 RPKI 在全球主流网站中的应用率, 以此对互联网基础设施 DNSSEC 与 RPKI 在全球互联网中的应用状况进行度量。通过分析得出, DNSSEC 的应用率约为 1.6%, 尤其以美国的部署发达程度最高; 同时, RPKI 技术体系自 2012 年提出以来, 其应用率已达到 6.4%, 并以欧洲地区的 RPKI 部署发达程度最高。

然而在 DNSSEC 与 RPKI 的部署实施过程中, 仍然存在若干因素制约其应用和部署。

DNSSEC 方面, 首先, DNSSEC 添加数字签名使 DNS 系统的查询和响应时延增大, 降低了网络性能; 其次, DNSSEC 所需密钥的产生和校验需要 CPU 计算能力做保障, 因此需要升级相关的网络设备、DNS 软件, 这无疑增加了 DNS 运营和使用的成本; 最后, 由于 DNS 面临的安全威胁并不仅是 DNS 欺骗攻击, 对于拒绝服务攻击、钓鱼攻击等网络安全威胁, DNSSEC 并不能提供有效的解决方案。

RPKI 方面, 首先, 缺乏 CA 资源分配误操作 (如 CA 证书的错误签发、ROA 数字签名对象的误签发) 的有效防御机制, 而上述误操作极易导致互联网的大面积宕机; 其次, 各大 RIR 及 NIR 所使用的 RPKI 软件各不相同, 缺乏对各方软件

的兼容性测试；最后，在互联网码号资源分配过程中，存在一些特殊资源分配场景，如中国 ISP 的码号资源分配自 CNNIC 和 APNIC，而 RPKI 体系尚未证明对于该场景的兼容性。

作为大规模改造互联网基础资源管理的协议框架，RPKI 与 DNSSEC 对现有的互联网名址技术体系具有较大的影响，其大规模部署可能存在的安全、可扩展和效率等多方面的问题事关我国网络基础设施的安全稳定，亟需对其关键技术进行深入研究和提前布局。

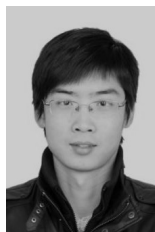
参考文献：

- [1] ERMAN, BENLI, HANDE, et al. Optimality condition of place of injury rule in cross-border internet torts and implications for turkey[J]. US-China Law Review, 2014, 411(10):1315-1321.
- [2] 朱韵成. YouTube 全球受阻两小时的背后[J]. 中国教育网络, 2008(4):26-27.
ZHU Y C. The whole truth of YouTube was has been blocked two hours[J]. China Education Network, 2008(4):26-27.
- [3] SOSNOVICH A, GRUMBERG O, NAKIBLY G. Analyzing Internet routing security using model checking[M]//Logic for Programming, Artificial Intelligence, Reasoning. 2015.
- [4] 刘宇靖. 互联网域间路由系统生存性研究[D]. 长沙: 国防科学技术大学, 2013.
LIU Y J. Study of the Internet inter-domain routing system survivability[D]. Changsha: National University of Defense Technology, 2013.
- [5] SCHLAMP J, HOLZ R, JACQUEMART Q, et al. HEAP: reliable assessment of BGP hijacking attacks[J]. IEEE Journal on Selected Areas in Communications, 2016, 34(6):1849-1861.
- [6] BALLANI H, FRANCIS P, ZHANG X. A study of prefix hijacking and interception in the Internet[C]//Conference on Applications, Technologies, Architectures and Protocols for Computer Communications. 2007:65-276.
- [7] 崔淑田, 刘越. DNSSEC 技术发展及影响分析[J]. 电信科学, 2012, 28(9):100-105.
CUI S T, LIU Y. The development and influence analysis of DNSSEC[J]. Telecommunications Science, 2012, 28(9):100-105.
- [8] 刘晓伟, 延志伟, 耿光刚, 等. RPKI 中 CA 资源分配风险及防护技术[J]. 计算机系统应用, 2016, 25(8):16-22.
- LIU X W, YAN Z W, GENG G G, et al. CA resource allocation risk and protective technique in RPKI[J]. Computer Systems and Application, 2016, 25(8):16-22.
- [9] LEPINSKIM, KENTS. An infrastructure to support secure Internet routing[S]. IETF RFC, 2012.
- [10] LEPINSKIM, KENTS, KONG D. A profile for route origin authorizations (ROA)[S]. IETF RFC, 2012.
- [11] WAEHLISCH M. Resource public key infrastructure (RPKI) router implementation[R]. 2014.
- [12] RPKI local trust anchor use cases[DB/OL]. <https://tools.ietf.org/html/draft-ymbk-lta-use-cases-00>.
- [13] IAMARTINO D, PELSSER C, BUSH R. Measuring BGP route origin registration and validation[M]//Passive and Active Measurement. Berlin: Springer International Publishing, 2015:28-40.
- [14] HUSTONG, MICHAELSONG. Validation of route origination using the resource certificate public key infrastructure (PKI) and route origin authorizations (ROAs)[S]. IETF RFC, 2012.

作者简介：



王翠翠 (1986-)，女，山东潍坊人，中国互联网络信息中心助理研究员，主要研究方向为互联网基础资源安全、BGP 安全机制、区块链技术。



延志伟 (1985-)，男，山西兴县人，博士，中国互联网络信息中心副研究员，主要研究方向为 IPv6 移动性管理、BGP 安全机制、信息中心网络架构。



耿光刚 (1980-)，男，山东泰安人，博士，中国互联网络信息中心研究员，主要研究方向为机器学习、大数据分析和互联网基础资源安全。