边界网关协议安全研究综述

王 娜 杜学绘 王文娟 刘敖迪

(解放军信息工程大学 郑州 450001)

(数学工程与先进计算国家重点实验室 郑州 450001)

摘 要 边界网关协议(the Border Gateway Protocol,BGP)是互联网事实上的域间路由标准协议.因 BGP 的安全脆弱性,互联网路由基础设施易受到攻击,破坏了互联网的网络可达性.从而,安全 BGP 对于整个互联网的可靠稳定运行具有重要意义.该文对近年来的 BGP 安全研究现状进行了梳理.首先,清晰界定了 BGP 威胁模型,从路由信息非真和路由传播非法的角度,将 BGP 面临的异常路由通告攻击分为前缀劫持、路径伪造和路由泄露这 3 类,阐述了攻击原理,给出了攻击实例;然后,梳理了 BGP 安全研究脉络,主要分为 BGP 安全防护和 BGP 异常检测两个研究方向,BGP 安全防护的研究内容主要包括针对前缀劫持与路径伪造的安全扩展和安全外包技术、路由泄露防护技术,BGP 异常检测的研究内容主要包括前缀劫持、路径伪造与路由泄露检测技术、主动响应技术、异常检测系统和 BGP 可视化工具.该文对上述研究点的主要思想、关键和难点问题、具体机制或方案的原理以及存在的不足等内容进行了深入、翔实的阐述和全面地分析、比较.最后,探讨了 BGP 安全研究面临的挑战,指出在安全防护、异常检测、域间路由信任和域间路由系统测量等 4 个方面需要深入研究的内容.该文研究可为相关研究人员和网络安全专家提供参考和借鉴,有助于 BGP 安全问题的理解和研究的深入.

关键词 BGP 安全;域间路由安全;前缀劫持;路由泄露;异常检测

中图法分类号 TP309 **DOI 号** 10.11897/SP.J.1016.2017.01626

A Survey of the Border Gateway Protocol Security

WANG Na DU Xue-Hui WANG Wen-Juan LIU Ao-Di

(*The PLA Information Engineering University, Zhengzhou* 450001)

(*State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou* 450001)

Abstract The Border Gateway Protocol (BGP) is the de facto interdomain routing protocol of the Internet. For the lack of effective security measures in BGP, the routing infrastructure of the Internet is vulnerable to various forms of attack, which will lead to disruption to network reachability on Internet. As a result it is highly important for Internet to secure BGP. The paper reviews recent research progress on BGP security. Firstly, the paper defines BGP threat model, where abnormal routing announcement attack to BGP is divided into prefix hijacking, path forging and routing leak, from the perspective of forged routing information and illegally route propogating, and describes attack principles, gives typical living examples. And then, the paper hackles research directions on BGP security, which mainly consists of security protection and anomaly detection, and the main research contents of BGP security protection include security extension and outsourcing techniques to defend prefix hijacking and path forging, and security protection techniques to defend routing leaking, the main research contents of BGP anomaly detection include detection techniques to prefix hijacking, path forging and routing leaking, active response techniques, anomaly detection

收稿日期:2016-04-21;在线出版日期:2016-09-20.本课题得到国家"八六三"高技术研究发展计划项目基金(2015AA011705)、河南省自然科学基金项目(No.162300410334)资助.**王 娜**,女,1980 年生,博士,副教授,主要研究方向为网络与信息安全.E-mail:tinatwf@163.com.**杜学绘**,女,1968 年生,博士,教授,主要研究领域为信息系统安全.**王文娟**,女,1981 年生,博士研究生,主要研究方向为网络安全.**刘敖迪**,男,1992 年生,硕士研究生,主要研究方向为网络安全.

systems and BGP visualization tools. The paper does thoroughly and detailedly expounding, and comprehensively analysis and comparison on main ideas, key and difficult issues, the principles and shortcomings of specific mechanisms or solutions of these research points. Finally, the paper discusses and analyses research challenges on BGP security, and points out some future works to be done in terms of security protection, anomaly detection, interdomain routing trust and interdomain routing system measurement. This survey provides the basis and reference for relevant researchers and network security experts to understand BGP security problems and promote in-depth research on BGP security.

Keywords　BGP security; inter-domain routing security; prefix hijacking; routing leak; anomaly detection

1　引　言

作为互联网事实上的域间路由标准协议，边界网关协议(Border Gateway Protocol，BGP)的安全性对于整个互联网的可靠稳定运行具有重要意义.然而，BGP 协议存在安全缺陷[1-2]，易受到前缀劫持、路径伪造和路由泄露等异常路由通告攻击.通过这些攻击，攻击者可劫持到达受害网络的数据流，形成流量黑洞，使受害网络“掉线”，造成全球网络的不稳定甚至瘫痪，或者窃听数据流，以及隐藏真实身份，以发送非法数据流(如垃圾邮件)等[2-5].有研究人员在深入分析全球路由数据后，指出实际中 BGP 异常路由通告攻击发生非常频繁[6].

鉴于 BGP 安全问题的重要性和严重性，IETF 在 2006 年成立了安全域间路由(Secure Inter-Domain Routing，SIDR)工作组①，专门从事 BGP 安全研究和相关标准的制定.在学术界，BGP 安全也是网络安全领域的一个重要研究方向.顶级会议 ACM SIGCOMM 自 2002 年始，几乎每年都会发表 1～2 篇与 BGP 安全相关的研究论文(如图 1 所示).但是，从第一个 BGP 安全方案 S-BGP 的提出至今已经有近 20 年的时间，BGP 安全问题仍然没有完全解决[7].这充分说明了 BGP 安全问题的复杂性和挑战性.

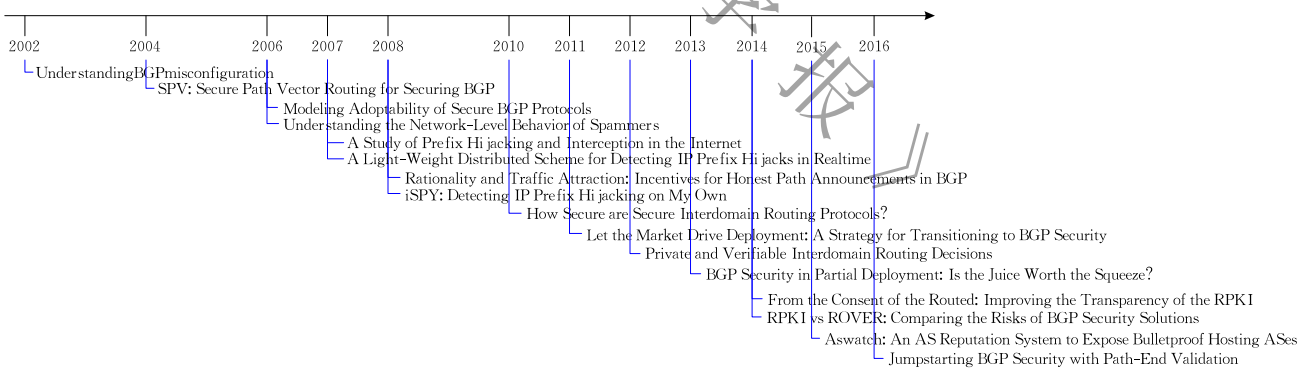


图 1　ACM SIGCOMM 自 2002 年起发表的 BGP 安全论文

基于此，本文对 BGP 安全威胁和安全研究现状进行了系统、科学的梳理，以为相关研究人员和网络安全专家提供借鉴，有助于该问题研究的深入和解决.本文具体工作如下：

(1)界定了 BGP 威胁模型，从路由信息非真和路由传播非法的角度，将 BGP 面临的异常路由通告攻击分为前缀劫持、路径伪造和路由泄露这 3 类，并且分别阐述了攻击原理，给出了攻击实例.

(2)系统梳理了 BGP 安全研究脉络(如图 2 所示)，主要分为 BGP 安全防护和 BGP 异常检测两个研究方向，其中，BGP 安全防护的研究内容主要包括针对前缀劫持与路径伪造的安全扩展和安全外包技术、路由泄露防护技术，BGP 异常检测的研究内容主要包括前缀劫持、路径伪造与路由泄露检测技术、主动响应技术、异常检测系统和 BGP 可视化工具.

(3)根据梳理的研究脉络，对这些研究点的主要思想，需要解决的关键和难点问题，具体机制或方

① IETF SIDR Workgroup. http://datatracker.ietf.org/wg/sidr, 2016.5.9

图 2 BGP 安全研究脉络

案的原理以及面临的挑战等内容，进行了深入、翔实的阐述，并对其中的重要研究点，针对前缀劫持与路径伪造的安全防护技术和前缀劫持检测技术，进行了全面的分析、比较.

(4) 探讨了 BGP 安全研究面临的挑战，指出在安全防护、异常检测、域间路由信任和域间路由系统测量等 4 个方面需要深入研究的内容.

本文第 2 节简要介绍 BGP 安全相关的背景知识；第 3 节阐述 BGP 威胁模型；第 4 节阐述 BGP 安全的研究现状；第 5 节探讨和展望 BGP 安全的研究挑战和未来研究方向；最后第 6 节总结全文.

2 背景知识

2.1 自治系统间关系

根据存在物理通信连接的自治系统(Autonomous System，AS)间的商业关系，ASes 间关系一般分为以下 3 类：

(1) transit(传输)关系，包括 customer-provider 和 provider-customer 两类. 若 ASes 间存在 transit 关系，则 provider AS 为 customer AS 提供付费的流量传输服务，customer AS 通过 provider AS 连接到互联网.

(2) peer(对等体)关系，即 peer-peer 关系. 若 ASes 间存在 peer 关系，则 peer ASes 间免费交换彼此网络(包括其客户网络)的流量.

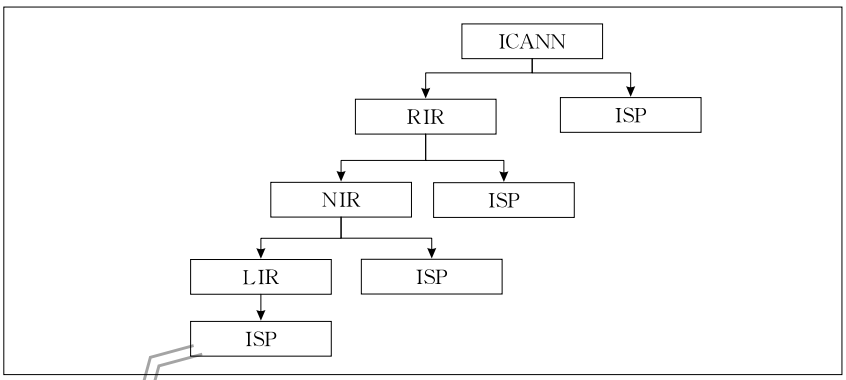
(3) sibling(成员)关系，即 sibling-sibling 关系. 若 ASes 间存在 sibling 关系，则 sibling ASes 属于相同机构，可免费交换流量.

除上述关系外，ASes 间还存在 hybrid(混合)和 partial-transit(局部传输)等复杂关系[70]. 其中，hybrid关系指若某 ASes 间同时存在 transit 和 peer 关系，则该 ASes 间存在 hybrid 关系；partial-transit 关系指若某 ASes 间存在 transit 关系但是 provider AS 只为 customer AS 提供到其 customer 和 peer ASes 的流量传输服务，则该 ASes 间存在 partial-

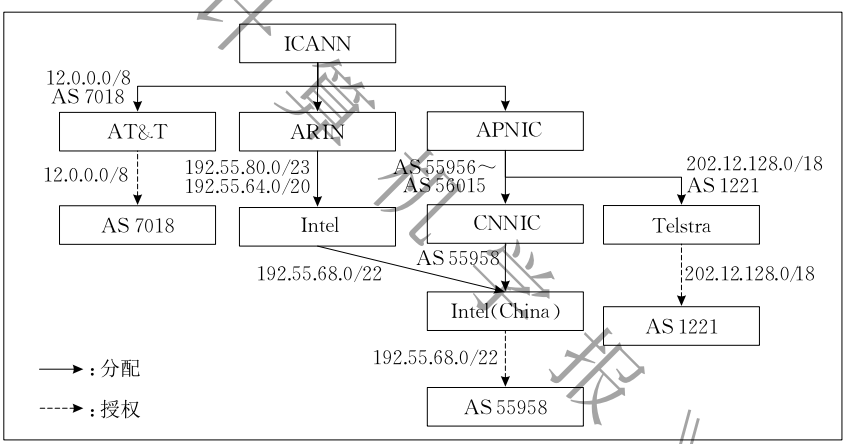
transit 关系.根据文献[70]分析,这些复杂关系只占 transit 关系的 4.5%,故本文不予考虑.

2.2　自治系统与 IP 前缀

互联网号码资源(如 AS 号码、IP 地址等)分配遵循从互联网名称和数字地址分配机构(The Internet Corporation for Assigned Names and Numbers, ICANN)到地区性 Internet 注册机构(Regional Internet Registry, RIR)、国家 Internet 注册机构(National Internet Registry, NIR)/本地 Internet 注册机构(Local Internet Registry, LIR)和互联网服务提供商(Internet Service Provider, ISP)的层次分配结构(如图 3 所示).



(a) 互联网号码资源分配层次结构



(b) 互联网号码资源分配实例

图 3　互联网号码资源分配

若某个 ISP 机构从 NIR/LIR 处分别申请获得 IP 前缀 p 和 AS 号码 a,且授权在 a 标识的 AS 内使用前缀 p'($p' \subseteq p$),则称 AS a“拥有”前缀 p'(即该 ISP 机构授权 AS a 可发起前缀 p'可达的路由通告),或 AS a 是 p'的合法源(origin)AS.

2.3　路由策略

自治系统的域间路由策略包括.

(1)最优路径选择策略. AS 收到路由通告后,根据最优路径选择策略,选择最优路径.该策略主要包括 LP(Local Preference)策略:由 customer 邻居转发的路径优于 peer 邻居,由 peer 邻居转发的路径优于 provider 邻居[71];SP(Shortest Paths)策略:优选路径属性 AS_PATH 长度最短的路径;TB(Tie Break)策略:优选下跳 AS 号码最小的路径.上述策略的优先级关系是“LP>SP>TB”.

(2)路由出站策略. AS 遵循路由出站策略向邻居传播路由通告.该策略基于 Gao-Rexford(GR)约束[72]的扩展,即 AS 将向所有邻居通告所有路径,除非其违背 GR 约束. GR 约束指如果 AS v_i 和/或 AS v_j 是 AS v_k 的客户,v_k 将向 v_i 传播由 v_j 通告的路由(其中 $i \neq j \neq k$).

2.4　BGP 安全脆弱性

根据 IETF RFC 4272[1],BGP 协议存在下述安全脆弱性:

(1) BGP 没有保障对等体间通信报文的完整性、新鲜性和对等实体的真实性.

(2) BGP 没有验证 AS 可发起网络层可达性信息(Network Layer Reachability Information, NLRI)

的权限.根据2.2节内容,AS只有获得前缀拥有机构的授权,才能够发起该前缀可达的路由通告.因此,收到路由报文的BGP路由器应该验证报文中源AS是否具有发起NLRI(即IP前缀)的权限.否则,AS可发起任意前缀可达的路由通告,从而,导致前缀劫持攻击(详见第3.1节).BGP没有提供相应的权限验证机制,存在安全脆弱性.

(3)BGP没有保障AS通告路径属性的真实性.根据第2.3节内容,路由报文中路径属性AS_PATH的长度是BGP最优路径选择策略的第2优先策略.如果路由报文的AS_PATH被篡改,会导致次优路径被选为最优路径,造成用户数据流被重定向,发生路径伪造攻击(详见第3.2节).因此,需要保障AS通告路径属性,特别是AS_PATH属性的真实性.但是,BGP没有提供相应机制,存在安全脆弱性.

对第1个安全脆弱性,可采用TCP MD5[1]或TCP-AO[73]来保障报文完整性、新鲜性和对等实体的真实性.对第2、3个安全脆弱性的解决方法见本文第4节的讨论.

3 威胁模型

BGP协议易遭受异常路由通告攻击.异常路由通告攻击指自治系统因偶然(如管理员的配置错误)或恶意的原因而发起、传播包含非真路由信息,如NLRI、AS_PATH,或违反路由出站策略的路由通告.通过异常路由通告攻击,攻击者可劫持以受害网络为目的地的数据流,使数据流重定向,形成流量黑洞,造成全球网络的不稳定和瘫痪,或窃听数据流,甚至隐藏真实身份以掩盖从事的非法行为(如发送垃圾邮件等).异常路由通告攻击可分为前缀劫持、路径伪造和路由泄露这3类(如图4所示).下面将依次开展分析.

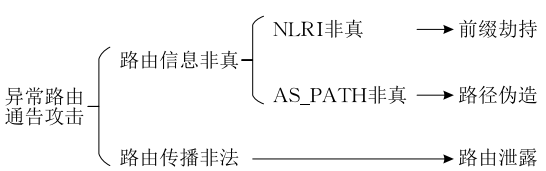


图4 异常路由通告攻击分类

3.1 前缀劫持

若某自治系统发起非本自治系统所拥有前缀(即NLRI非真)的可达路由通告,则称发生前缀劫持.前缀劫持由BGP协议第2个安全脆弱性导致.根据所劫持前缀的类型,前缀劫持可进一步分为regular前缀劫持、more specific前缀劫持和bogus前缀劫持这3类.若攻击AS发起受害AS拥有前缀的可达路由通告,则称发生regular前缀劫持;若攻击AS发起受害AS拥有前缀的more specific前缀的可达路由通告,则称发生more specific前缀劫持;若攻击AS非法发起未分配前缀的可达路由通告,则称发生bogus前缀劫持.不同类型前缀劫持造成的影响是不同的.如图5所示,因遵循最长前缀匹配原则,一般而言,more specific前缀劫持比regular前缀劫持吸引的数据流更多.2008年Pakistan telecom hijack YouTube事件①就是典型的more specific前缀劫持.垃圾邮件发送者经常通过劫持bogus前缀来发送垃圾邮件,如AS 28716(Italy ISP)在2009年11月13日到2010年1月15日近两个时间内持续劫持IPv6 bogus前缀d000::/8,却未被发现②.

3.2 路径伪造

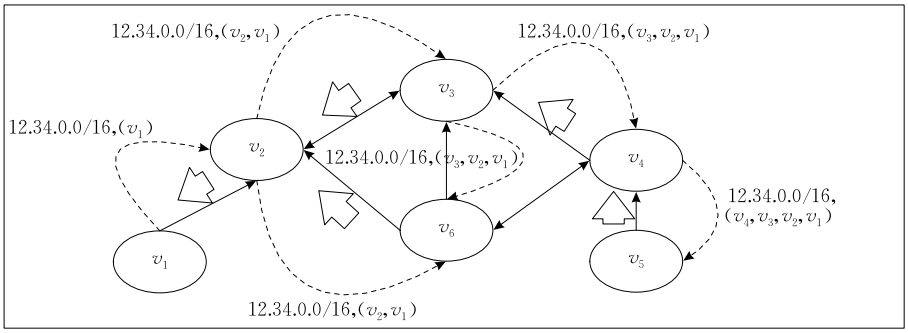
若某自治系统向邻居自治系统传播AS_PATH路径属性非真的路由通告,即攻击AS在对路由通告的AS_PATH属性进行删除、插入等篡改操作后,再将其传播给邻居AS,则称发生路径伪造.该攻击由BGP协议第3个安全脆弱性导致.鉴于SP最优路径选择策略,最常见的路径伪造攻击是AS_PATH缩短攻击(AS_PATH shortening).图6给出了一种典型的AS_PATH缩短攻击(又称为next-hop攻击).2011年Link Telecom事件是典型的next-hop攻击[74].与图5所示前缀劫持不同,图6中攻击者v_5劫持受害网络v_1的数据流后,仍然继续将其转发到v_1,并不破坏v_1的网络可达性.

3.3 路由泄露

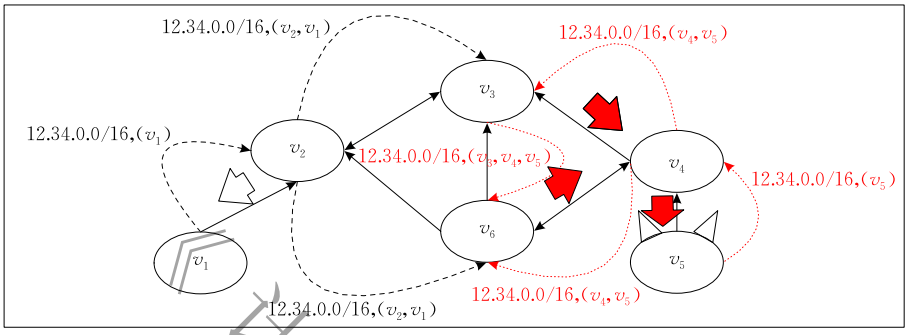
若自治系统向邻居自治系统传播违背路由出站策略的路由通告,即若AS收到peer或customer邻居传播的non-customer路由,则发生路由泄露.与前缀劫持和路径伪造不同,路由泄露具有"路由信息真实,路由传播非法"的特点.根据邻居间的商业关系,路由泄露主要包括peer路由泄露和customer路由泄露两类[75].peer路由泄露指攻击者向peer邻居传播其从peer和/或provider邻居获得的路由,如图7(a)所示;customer路由泄露指攻击者向

① Pakistan hijacks Youtube. http://www.renesys.com/blog/2008/02/pakistan_hijacks_youtube_1.shtml, 2008.2/2016.5.10

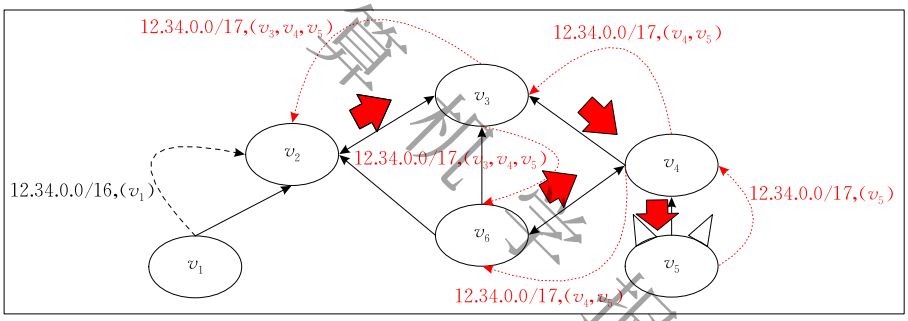
② Securing the Internet backbone: Current activities in the IETF's Secure Interdomain Routing Working Group. www.potaroo.net/presentations/2012-05-22-route-secure.pdf, 2012.5.22/2016.5.10



(a) 正常情况



(b) regular前缀劫持



(c) more specific前缀劫持

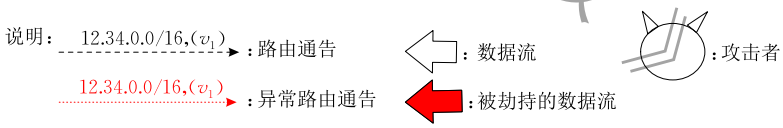


图 5　前缀劫持

provider 邻居传播其从 peer 和/或 provider 邻居获得的路由，如图 7(b)所示. 2012 年 Telstra-Dodo[①] 和 2015 年 Telekom Malaysia-Level 3[②] 等事件属于 customer 路由泄露，2012 年 Google-Moratel[③] 和 2015 年 Hathway-Google[④]等事件属于 peer 路由泄露.

4　BGP 安全方案

根据不同的安全思想，BGP 安全方案可分为安全防护和异常检测两类

4.1　安全防护

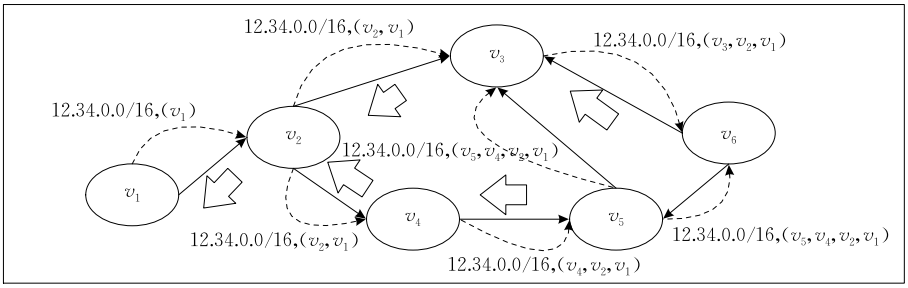
BGP 安全防护方案拟从根本上解决 BGP 安全问题，一直是 BGP 安全研究的主要方向. 如图 2 所示，因为不同的攻击原理，BGP 安全防护可分为针对前缀劫持与路由伪造的安全防护和针对路由泄露的安全防护. 根据与 BGP 的耦合关系，针对前缀劫持与路径伪造的安全防护可进一步分为与 BGP 紧耦合的安全扩展技术和与 BGP 松耦合的安全外包

① Huston G. Leaking routes. http://www.potaroo.net/ispcol/2012-03/leaks.html, 2012.3/2016.5.10

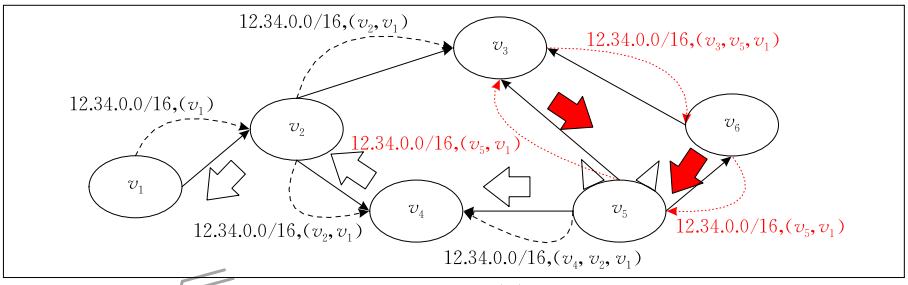
② Toonk A. Massive route leak causes Internet slowdown. http://www.bgpmon.net/massive-route-leak-cause-internet-slowdown/, 2015.6/2016.5.10

③ Paseka T. Why Google Went Offline Today and a Bit about How the Internet Works. https://blog.cloudflare.com/why-google-went-offline-today-and-a-bit-about/, 2012.11.6/2016.5.10

④ Toonk A. What caused the Google service interruption. http://www.bgpmon.net/what-caused-the-google-service-interruption/, 2015.3.12/2016.5.10

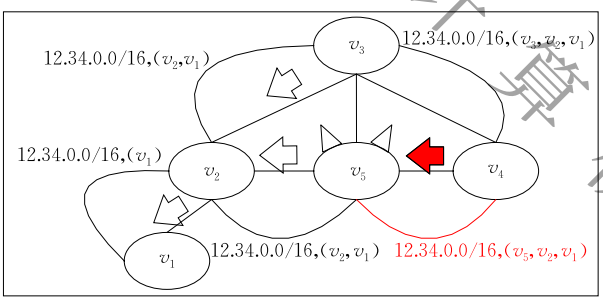


(a) 正常情况

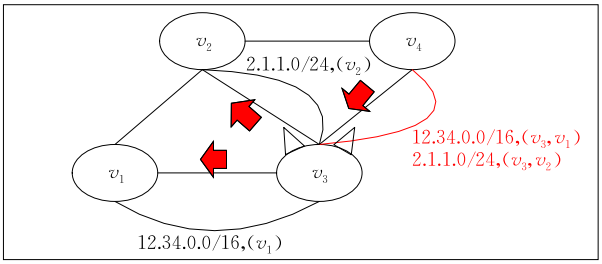


(b) next-hop攻击

图 6 路径伪造



(a) peer路由泄露



(b) customer路由泄露

图 7 路由泄露

技术. 更进一步地,安全扩展技术可分为 S-BGP 优化和以 S-BGP 为基础的 RPKI&ROA&BGPsec,而根据不同的优化方法,S-BGP 优化方法又进一步分为基于有效的密码技术、分布式信任和域间路由系统演化特征的优化方法. 下面将进行详细阐述.

4.1.1 针对前缀劫持与路径伪造的安全防护

4.1.1.1 安全扩展技术

安全扩展技术的主要思想是扩展 BGP 协议,采用数字签名等密码技术提供源自治系统的权限证明和 AS_PATH 路径属性的真实性保障,以防止前缀劫持和路径伪造攻击的发生. 在 1997 年,BBN 技术首次提出第 1 个 BGP 安全解决方案 S-BGP[76] 后,该技术的研究就分为两个阶段,第 1 阶段主要研究如何优化 S-BGP,以降低其计算、存储开销[8-9,17-19,77-80] 和密钥管理复杂度[10-12,14-16];在 2012 年 IETF SIDR 工作组以 S-BGP 为基础提出资源公钥基础设施(Resource Public Key Infrastructure,RPKI)、路由源授权(Route Origin Authorizations,ROA)和 BGPsec 后,该技术的研究就围绕 RPKI、ROA 和 BGPsec 的标准化[20-22,81-83]、安全问题与改进[84-88]、实现[89-90]、监测工具①②③④⑤、部署测量[91-95] 及策略[96-97] 等内容展开.

(1) S-BGP 的优化

S-BGP 与下节阐述的 RPKI&ROA&BGPsec 原理相同,这里不再赘述. S-BGP 面临计算、存储开销大,需更新路由器软、硬件和部署全网覆盖的集中式公钥基础设施(Public Key Infrastructure,PKI)等挑战[4]. 基于此,大量优化方案被提出. 优化方案可分为以下几类.

① 基于有效的密码技术实现优化

为了降低 S-BGP 路径认证的计算和存储开销,

① RPKI spider. http://rpkispider.verisignlabs.com/, 2016.5.16
② LACNIC. RPKI looking glass. www.labs.lacnic.net/rpki-tools/looking_glass/, 2016.5.16
③ NIST. RPKI deployment monitor. http://www-x.antd.nist.gov/rpki-monitor/, 2016.5.16
④ RIPE. RPKI validator. http://localcert.ripe.net:8088/trust-anchors, 2016.5.16
⑤ Surfnet. RPKI dashboard. http://rpki.surfnet.nl/validitytables.html, 2016.5.16

SPV(Secure Path Vector)[8]和 APA(Aggregated Path Authentication)机制[9]分别探讨了采用不同密码技术的优化方案.

SPV 机制探索了采用对称密码算法实现 AS_PATH 路径认证的可行性.该机制采用一次性签名机制生成 AS_PATH 签名,引入新的路径属性 AS-PATH protector 来携带该签名,且采用哈希树实现一次性签名的验证和单向哈希链来缩减 AS_PATH protector 的长度.SPV 是轻量级的.但是,因为机制的假设条件过于理想,在真实互联网环境下,SPV 的安全性、可扩展性和性能都受到质疑[80].

APA 机制基于时间有效的签名分摊(signature amortisation)方法和空间有效的聚合签名(aggregate signature)方法,提出一组聚合路径认证的构建方法.签名分摊方法使发送给多个 BGP 邻居的相同路由通告只需要签名一次,降低了密码操作的延迟,加快了 BGP 的收敛速度;聚合签名方法可将对 AS_PATH 的多个签名聚合成一个签名,接收者只要验证该聚合签名就可判断被聚合多个签名的真实性,缩短了 BGP 报文的长度,降低了路由器的存储开销.为了进一步降低存储开销,文献[79]还提出了一种支持延迟验证(lazy verification)的序列聚合签名方法,该方法允许签名者直接增加自己的签名到未验证的聚合签名上,且延迟签名验证直到负载允许或已获得必要的公钥信息.

不同于基于证书的密码体制,基于身份的密码体制将用户的身份信息作为公钥,可消除基于证书密码体制面临的证书管理负担.鉴于此,有些方案[10-13]将基于身份的密码机制引入 BGP 安全.例如,id²r 方案[11]提出基于地址分配路径长度的源 AS 认证机制和基于身份聚合签名算法的路径认证机制,以及一种分布式层次密钥分发协议,以解决基于身份密码系统固有的密钥托管问题.与 S-BGP 相比,id²r 避免了建立、管理 PKI 的负担,减少了路由器的计算和存储开销,且可抵抗上层 ISP 前缀劫持攻击[98].文献[12]提出了一个基于身份的密钥基础设施 iPKI,该设施基于 IP 地址分配层次结构,以 IP 前缀自证明 IP(self-attested IP,sIP)为公钥,在向下层分配 IP 前缀时,同时生成与该 IP 前缀对应的私钥;在 iPKI 基础上,文献[12]进一步提出 IBSOV(In-Band Self Origin Verification)协议,该协议基于 sIP 地址和地址授权证明 sROA(self Route Origin Authorization)来实现前缀的源认证,iPKI 降低了身份密钥协商的复杂度和开销.

②基于分布式信任实现优化

由思科公司在 2003 年提出的 soBGP(secure origin BGP)方案[14]也是一个典型的 BGP 安全解决方案.与 S-BGP 不同,soBGP 仅基于 AS 的公钥证书 EntityCert,且采用分布式网状信任(web of trust)模型管理 EntityCert;采用由源 AS 签名生成的源 AS 证明 AuthCert,实现源 AS 和前缀的绑定(如图 8 所示);采用 ASPolicyCert 实现 AS_PATH 验证,具体方法是每个 AS 在其自签名的 ASPolicyCert 中列出自己的邻居 AS,当邻居间分别在 ASPolicyCert 证书中列出彼此时,认为该邻居间存在直接路径,基于 ASPolicyCert 可构建出网络的 AS 拓扑图(无向图),通过验证路由通告的 AS_PATH 在拓扑图中是否存在就可实现 AS_PATH 路径验证.需要指出的是 web of trust 信任模型没有体现出 AS 号码的分配和指派,且即使路由通告中的 AS_PATH 路径属性在网络 AS 拓扑图中存在,也不意味着该路径属性真实.因此,与 S-BGP 相比,soBGP 是一个以牺牲安全性来获得性能提升的轻量级方案,避免了对互联网号码资源集中层次式分配结构的依赖,且拥有支持增量式部署的灵活部署选项,易于部署实现.但是,soBGP 还遗留了若干问题,包括需要度量 web of trust 模型中不同 AS 的信任度,以反应其签名公钥证书 EntityCert 的可信性;验证 AuthCert 时,需要确定 EntityCert 的信任锚和根据模糊的地址权限派生关系,确定最终的可信地址授权者(如表 1 所示);以及在网络拓扑发生变化时如何及时更新 ASPolicyCert 等.

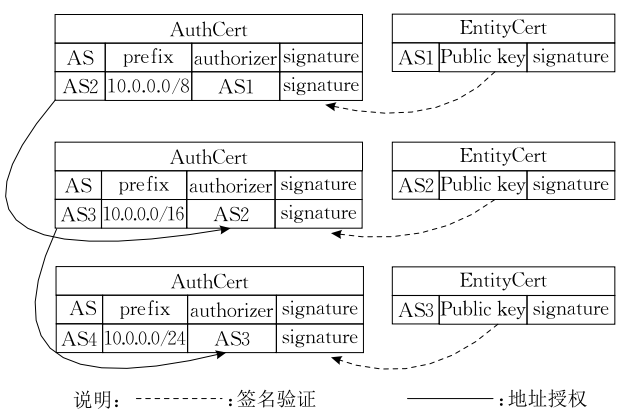


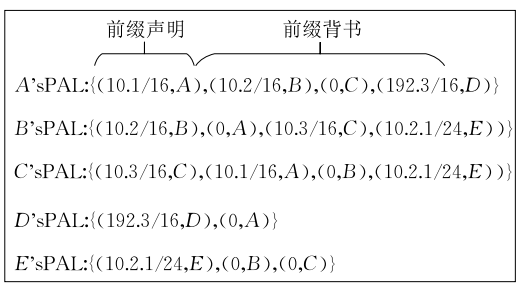
图 8　soBGP 中 AuthCert 与 EntityCert 关系

psBGP(pretty security BGP)机制[15]摒弃了 S-BGP 中对庞大地址证书的管理,采用与其相似的层次式 PKI 结构实现相对少量 AS 证书的管理,以降低密钥管理的负担;引入AS评价机制,并在此基

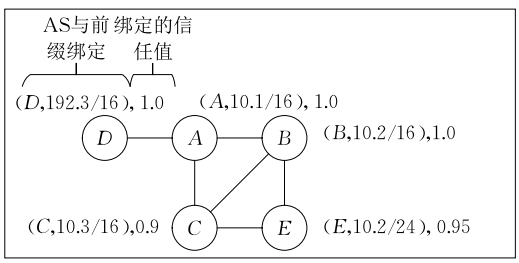
表 1 soBGP 源认证步骤

soBGP 源认证步骤
1. 验证源 AS 的 AuthCert
1-1. 获取 AuthCert 中 authorizer(如图 5 中 AS3)的 EntityCert;
1-2. EntityCert 在有效期内,且没有被撤销;
1-3. 确定信任锚,构建 EntityCert 的证书链,验证 EntityCert 的真实性;
1-3-1. 上级证书的公钥可验证下级证书的签名;
1-3-2. 上级证书的主体是下级证书的发布者;
1-4. 使用 EntityCert 的公钥验证 AuthCert 的签名.
2. 重复下述过程,直至 AuthCert 中的 authorizer 是可信任的地址授权者;
2-1. 获取 AuthCert 中 authorizer 的 AuthCert 证书(如图 7 中 AS3 的 AuthCert 证书);
2-2. 采用步骤 1 中方法验证 authorizer 的 AuthCert;
2-3. authorizer 的 AuthCert 证书中 prefix 包含被授权 AS AuthCert 证书中 prefix.

础上,实现基于分布式信任的前缀源 AS 认证和 AS_PATH 路径认证. 具体地,psBGP 中,每个 AS 签名生成一个前缀声明列表(Prefix Assertion List, PAL),该列表包含本 AS 所拥有前缀的声明和对其邻居 AS 所拥有前缀的背书;基于对网络中 AS 的评价和这些 ASes 生成的 PALs,构建 AS 前缀图(AS prefix graph)(如图 9 所示),该图标注了网络中 AS 间的连接关系、AS 和前缀的绑定关系以及对该绑定关系的信任度. 如果某 AS 和前缀绑定的信任度高于阈值,或该前缀已由源 AS 声明且超过一定数目 ASes 背书,则认为该绑定关系真实,实现前缀源认证. psBGP 采用与 BGPsec 相似的路径认证机制,但是其允许只有 AS_PATH 中一部分 AS 提供路径签名,并且提出一个阶梯路径认证方法,即基于对签名路径 AS 的评价和 AS_ PATH 中部分或全部路径签名,计算 AS_PATH 的信任度,若该信任度高于阈值则认为路径真实. 此方法允许验证路由器在性能和安全性之间进行取舍. 若路由器的计算资源有限,则可设置较低阈值(即只需验证少量路径签名),以安全性的降低换取性能的提升. 与 S-BGP 相比,psBGP 只需部署相对简单的 AS 证书 PKI,避免了部署复杂地址证书 PKI 带来的管理负担;引入分布式信任,基于 AS 评价机制,提出前缀源认证的分布式方法和阶梯路径认证方法,降低了计算和存储开销;并且,在 BGP 安全方案的增量式部署方面进行了有益的探索. 但是,psBGP 也面临若干挑战,包括如何实现 AS 间评价?如何避免针对前缀源认证的 AS 共谋攻击?前缀源认证时,所有提供前缀背书的 AS 一视同仁是否恰当?以及构建 AS 前缀图时,冲突 PALs 的处理方法等.



(a) 前缀声明列表



(b) D的AS前缀图

图 9 AS 前缀图示例
(其中,D 对 A,B,C 和 E 的评价分别为 1,0.5,0.8 和 0.5)

基于互联网 AS 结构 Rich-Club 特性的观察,SE-BGP(Security Enhanced BGP)机制[16]提出 AS 联盟的概念,并采用一种分布式信任模型 TTM(Translator Trust Model),建立基于 AS 联盟的安全体系结构,以降低系统证书规模,简化 S-BGP 中复杂的密钥管理.

③ 基于域间路由系统演化特征实现优化

作为一个复杂系统[99],域间路由系统自发演化出若干特征,基于这些特征可有针对性地设计优化方案. 通过分析一年内来源于 RouteViews① 40 个观测点的 BGP 路由数据,文献[17]观察到在一个月内低于 2%前缀在 10 条以上路径上通告,低于 0.06%的前缀在 20 条以上路径上通告,即 BGP 路径具有有限差异性和高稳定性的特点;在该观察基础上,该文提出了一组路径认证优化机制,包括基于哈希链的列表路径认证和基于 Merkle 哈希数的树路径认证等,以降低 S-BGP 路径认证的计算开销. FS-BGP(Fast Secure BGP)[18]观察到域间路由具有"基于邻居的路由策略"传播特征,因此可通过签名路径中相邻 AS 三元组来实施路径认证,避免盲目签名整条 AS_PATH 路径带来的高开销问题. OA(Origin Authentication)机制[19]发现互联网 IPv4 地址分配是稳定和紧凑的,提出基于 Merkle 哈希树构建分配路径证明实现在线源认证的方法,仿真结果显示在理想情况下该方法是可行的,且计算开销得到显著降低.

① Route Views Project. http://www.routeviews.org/, 2016.5.10

(2) RPKI&ROA&BGPsec

① RPKI&ROA&BGPsec 的原理

RPKI 是依托互联网号码资源分配层次结构构建的一个公钥基础设施，实现资源证书的管理(如图 10 所示). 资源证书与公钥证书的区别在于它不仅实现证书主体与公钥的绑定，而且体现互联网号码资源的指派. 资源证书与互联网号码资源分配中一次资源的分配或指派相对应. 当上层机构为下层机构分配 IP 地址/AS 号码时，上层机构为其生成的资源证书称为 CA 证书. 当机构指派资源的使用时，生成的资源证书称为 EE(End Entity)证书. EE 证书分为前缀证书和路由器证书. 前缀证书指当机构的某 IP 前缀被指派使用时，生成包含该 IP 前缀的 EE 证书. 路由器证书指当 AS 内某 BGP 路由器被指派代表该 AS 传播路由通告时，生成该路由器的 EE 证书. CA 证书和 EE 证书通过扩展 X.509 证书格式实现，主要包括 IP 地址/AS 号码/路由器标识及其相应公钥等相关信息，以证明机构对这些互联网号码资源的所有权.

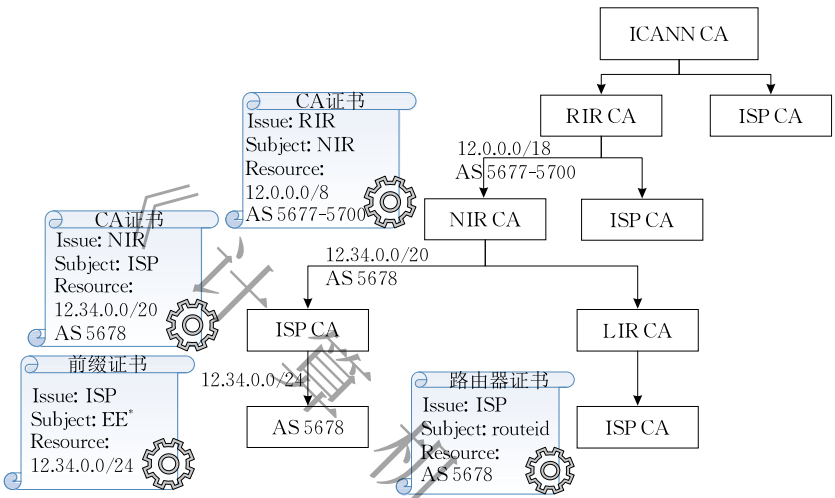


图 10　RPKI 结构示例

在“仅当 ISP 机构授权其所拥有的某 AS 使用某前缀时，该 AS 才能发起此前缀可达路由通告”的思想指导下，ROA 机制提供了 AS 的权限证明(即 ROA). ROA 由 ISP 采用前缀 p 的前缀证书对应私钥签名(p，AS a)生成，实现前缀 p 和 AS a 的绑定. 其它 AS 通过验证 ROA，实现路由通告中前缀源 AS 的认证. 验证 ROA 的具体方法是，首先采用如表 2 所示步骤验证 p 的前缀证书，其次使用 p 的前缀证书中公钥验证 ROA 的数字签名，若签名正确，且 ROA 中前缀包含在前缀证书的 IP 地址资源中，则 ROA 验证成功. 为了减少路由器的计算开销，IETF SIDR 工作组建议 ROA 机制与 BGP 解耦合，并采用外包的方法实现.

表 2　EE 证书验证步骤

EE 证书验证步骤
1. EE 证书在有效期内，且没有被撤销；
2. 确定信任锚(如 ICANN CA)，构建证书链，验证 EE 证书的真实性.
2-1. 上级 CA 的公钥可验证下级证书的签名；
2-2. 上级证书的主体是下级证书的发布者；
2-3. 下级证书的资源(如 AS 号码、IP 前缀)包含在上级证书的资源内.

为防护路径伪造攻击，BGPsec 机制中每个 AS 向下一跳 AS 传播路由通告时，同时提供路径证明，该证明采用一个数字签名序列实现. BGPsec 机制新增一个可选属性 BGPsec_Path 来携带路径证明. 如图 11 所示，当 AS b 向邻居 AS c 传播从 AS a 收到的路由通告时，AS b 对由收到报文 BGPsec_Path 中签名 $sig1$、本 AS 号码 b 和下一跳 AS 号码 c 构成的 $ap2$ 签名，生成 $sig2$，且在收到 BGPsec_Path 属性后新增内容($ap2$，$sig2$)，生成新的路由通告报文，发送给 AS c. 从而，当邻居 AS c 收到此路由通告后，依次使用 AS_PATH 中 AS 对应的路由器公钥验证 BGPsec_Path 属性中的数字签名列表，若全部验证成功，说明路由通告中的 AS_PATH 路径属性真实.

② RPKI 带来的安全挑战

RPKI 为 ROA 和 BGPsec 提供密钥管理功能，是保障 BGP 安全的支撑性基础设施. 但是，RPKI 采用“集中权威式”信任模型，以技术方式增加了 RPKI 中 CA 权威(如 RIR、NIR、ISP 等)的“权力”，使其能够“单方面”地改变 IP 前缀的状态，如从“valid”降级为“unknown”/“invalid”，或从“unknown”升级为“invalid”. 可采用的方法包括撤销、重写、删除或毁

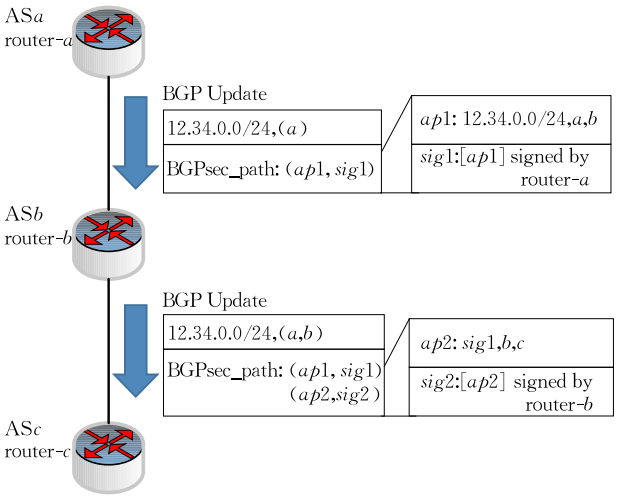


图 11 BGPsec 原理

坏已有的 RPKI 目标(资源证书和 ROA),发布新的 RPKI 目标等[84,87-88]. 例如,在 2013 年 12 月 13 日,一个绑定 173.251.0.0/17 和 AS 6128(maxlength=24)的 ROA 增加到以 ARIN 为根的实验 RPKI 中,导致网络中大量相关 IP 地址(如 AS 53725 的 173.251.91.0/24,AS 13599 的 173.251.54.0/24 等)的状态从"unknown"降级为"invalid".

根据 RFC6483 草案[21]规定,对 invalid 路由,路由器可采取 drop invalid 和 depref invalid 两种策略. drop invalid 策略严格但是难以实现故障保护,会因 RPKI 偶然故障而失去对 invalid 地址空间的网络访问,depref invalid 策略宽松,可实现故障保护,但是却不可避免地仍然面临 regular/more specific 前缀劫持攻击问题.

目前针对该挑战的解决思路分为两类:一是以技术方式降低 RPKI 中权威的权力,例如,在权威改变 IP 地址的状态时,Suspenders 机制[86]要求必须得到该地址拥有者的同意,文献[85]则要求得到该地址分配路径上所有权威的同意;二是采用监测工具实现对 RPKI 中权威"misbehave"行为的检测和报警,以及时发现会导致 IP 地址状态异常变化的行为.

另外,与 RPKI 相似,DNSSEC 和 web PKI 系统也采用集中式权威. 但是,近年来有充分的证据表明这些系统中的权威曾被攻击①②、发生过配置错误③,甚至迫于压力删除信息(如 DNS takedown[100])和为伪造信息提供证明[101]等. 因此,有理由相信 RPKI 权威也会面临相同问题.

4.1.1.2 安全外包技术

考虑到目前域间路由系统在可扩展性上面临的严峻挑战,安全扩展技术的有限增量式部署能力、高计算和存储开销、更新骨干路由器软、硬件的实际不可行性等,都严重影响了该技术的实际部署实现. 因此,安全外包技术被提出. 安全外包技术的主要思想是不修改 BGP 协议和路由器,外包解决 BGP 的安全问题. 典型技术包括 IRV(Interdomain Routing Validation)和 ROVER(Route Origin VERification).

(1) IRV

IRV 方案[23]通过在每个 AS 中部署一个 IRV 服务器来构建一个覆盖域间路由系统的分布式路由查询验证系统,实现路由与安全的分离,来避免增加域间路由系统的额外负担,且支持增量式部署. IRV 实现前缀源 AS 认证和路径认证的方法是,当路由器收到路由通告报文后,它将查询本地 IRV 服务器,本地 IRV 服务器将会进一步查询该路由通告源 AS 的 IRV 服务器,以进行前缀源 AS 认证;验证报文的 AS_PATH 路径属性时,本地 IRV 服务器可向 AS_PATH 路径中每个 AS 的 IRV 服务器进行查询,询问是否收到该路由通告,以及该路由通告的下一跳 AS 等信息. 而且,IRV 允许每个 AS 自主选择验证 AS_PATH 路径的时间和验证方式(如全部查询验证或仅查询验证部分 AS),以在安全和性能之间进行折中. 除了前缀源 AS 认证和路径认证,IRV 还提供实现敏感信息保护的路由策略可控查询功能. 正如文献[23]中所指出的,IRV 方案的有效运行必须解决路由器与 IRV 服务器间真实路由数据的同步问题、IRV 服务器的发现问题、IRV 服务器间通信的安全保障问题(包括新鲜性、完整性和通信源真实性等)以及网络不可达时 IRV 服务器间的通信问题等.

(2) ROVER

ROVER 方案[24]基于目前已有的反向 DNS 基础设施,引入新的编码机制,使用 DNS 反向查询来验证前缀源 AS 的真实性. ROVER 引入的新机制包括:① 命名约定,以唯一命名 IPv4 或 IPv6 前缀的

① Bright P. arstechnica: How the Comodo certicate fraud calls CA trust into question. http://arstechnica.com/security/2011/03/how-the-comodo-certificate-fraud-calls-ca-trust-into-question/, 2011.3.25/2016.5.16

② Galperin E, Schoen S, Eckersley P. A post mortem on the iranian DigiNotar attack. https://www.eff.org/deeplinks/2011/09/post-mortem-iranian-diginotar-attack, 2011.9.13/2016.5.16

③ Wisniewski C. Turkish certicate authority screwup leads to attempted google impersonation. https://nakedsecurity.sophos.com/2013/01/04/turkish-certificate-authority-screwup-leads-to-attempted-google-impersonation/, 2013.1.4/2016.5.16

DNS 名字；②Secure Route Origin(SRO)资源记录，以实现前缀与合法源 AS 的绑定，并采用 DNSSEC 签名保护；③Route Lock(RLOCK)记录，以指示某前缀是否使用 ROVER 方法保护. 从而，在收到路由通告后，ROVER 验证器可根据定义的命名约定将前缀转换成 DNS 名字，且发布对该名字 SRO 记录的查询，若返回 DNSSEC 认证的 SRO 记录验证有效，且 SRO 记录中 AS 与路由通告中的源 AS 匹配，则该路由通告中源 AS 合法；若 SRO 记录中 AS 与路由通告中的源 AS 不匹配，或没有查询到 SRO 记录，但是查询 RLOCK 记录被设置，则发生前缀劫持；若 SRO 记录的 DNSSEC 验证失败，或查询 SRO 和 RLOCK 记录都不存在时，则 ROVER 机制建议按照正常 BGP 操作，以实现“故障保护”，提高 ROVER 机制的适用性[102]. ISP 可通过 DNS 更新来实时增加或删除源 AS 信息，且在几分钟内全球就可访问到. 目前 ROVER Tested① 已经投入应用. 但是，到 2014 年 5 月仅有 0.5%的.com 和.net 域部署了 DNSSEC[58]，可见 ROVER 的未来部署前景并不明朗.

4.1.1.3　一些比较

本文从安全功能、密钥管理和性能这 3 个方面对上述典型机制和方案进行了比较(如表 3 所示).

表 3　针对前缀劫持和路径伪造的典型安全防护技术比较

	安全功能					密钥管理				性能		
	前缀劫持防护			路径伪造防护		密钥管理基础设施	密码体制	信任模型	密钥规模	计算开销*	存储开销*	网络开销*
	源认证与授权	源认证	源验证	路径认证	路径验证							
RPKI&-ROA&-BGPsec	√	—	—	√	—	Y	公钥	集中式	$r+s+t$	—	—	—
soBGP	—	√	—	—	√	Y	公钥	分布式	r	优	—	—
psBGP	—	—	√	√	—	Y	公钥	集中式	r	优	—	相当
OA	√	—	—	—	—	Y	建议采用 RPKI			优	—	—
SPV	—	—	—	√	—	Y	建议采用 RPKI			优	优	劣
APA	—	—	—	√	—	Y	建议采用 RPKI			优	优	优
FS-BGP	—	—	—	√	—	Y	建议采用 RPKI			优	—	—
id²r	—	√	—	√	—	Y	IBC	分布式	$r+t$	优	优	优
IRV	—	—	√	√	—		—			优	优	—
ROVER	√	—	—	—	—	N	—			优	优	—

注：* 表示与 S-BGP 的开销相比.

其中，源认证与授权指显式证明某前缀的分配路径和源 AS 获得了前缀拥有 ISP 的授权，源认证指隐式证明某前缀的分配路径和源 AS 的前缀发起权限，源验证指证明某 AS 以一定置信度是前缀的源 AS；路径认证指采用密码学或其它方法显式证明 AS_PATH 路径属性的真实性，路径验证指仅证明 AS_PATH 路径属性所标识路径的真实性. 因为性能开销与仿真环境紧密相关，为严谨起见，本文中的比较结果以相关论文结果为依据，没有列出论文中未涉及的性能.

4.1.2　针对路由泄露的安全防护

不同于前缀劫持和路由伪造，路由泄露中自治系统泄露的是真实的路由信息，只是违反了路由出站策略，即路由信息真实，路由传播非法. 因此，上述安全技术不能防止路由泄露[103]. IETF SIDR 工作组也将路由泄露问题委托给 IETF GROW(Global Routing Operations，全球路由操作)工作组②解决.

一般而言，使用路由过滤器就可实现对 customer 路由泄露的有效过滤. 研究显示如果所有 customer zone＞25 的 ASes 都正确部署了路由过滤器，可防止至少 48%的路由泄露[104]. 但是，在实际中维护一个准确的路由过滤器是困难的，特别对于大型 ISP 而言③；而且，路由过滤器仅对 customer 路由泄露有效.

目前路由泄露防护技术的主要思想是 AS 在向外传播路由通告时，增加一个标识信息，接收 AS 根据该信息就能够判断该路由传播是否合法. 需采用 BGPsec 机制来保护标识信息的真实性. 文献[25]提出当 AS 传播路由通告给 peer 或 customer 邻居时设置一个标记，从而当某 AS 从 customer 或 peer 邻居收到路由通告后通过验证该标记序列，就能够判断该路由通告是否违反路由出站策略；文献[25]还进一步指出该方法只在超过 60%的 ASes 都部署时，才会有效，但文中仅测试了 stub AS 泄露路由的情形. 文献[26-27]建议根据链路类型，对 AS_PATH 中每跳 AS-hop 着色，如若路由通告发送给 provider 邻居，AS-hop 着绿色，若发送给 peer 或 customer 邻居，AS-hop 着黄色，从而从 customer 邻居接收到的路由通告必须使所有 AS-hop 都着绿色，从 peer 邻

① BGP ROVER: Route Origin Verification. https://rover.secure64.com/, 2016.5.10

② IETF Global Routing Operations(GROW) Working Group. https://datatracker.ietf.org/wg/grow/, 2016.5.10

③ Huston G. Leaking routes. http://labs.apnic.net/?p=139, 2012.3.5/2016.5.16

居接收到的路由通告必须使除最后一跳是黄色外，其它都是绿色，否则就发生路由泄露. GRO 工作组提议在 BGPsec 签名中引入 Route Leak Protection (RLP)域，该域由发送 BGPsec 更新的 AS 设置，以指示接收 AS 是否允许向其 provider 或 peer 邻居通告此路由[28]. 例如，如果 RLP 设置为 00，那么接收 AS 能转发该更新到 provider 或 peer 邻居，而如果设置为 01，则接收 AS 不被允许转发该更新至 provider 或 peer 邻居. 从而，如果 AS 从 customer 邻居收到 RLP 域为 01 的路由更新，则说明发生路由泄露. 这类技术的主要局限是需要修改 BGP 协议，依赖于 BGPsec 来保障真实性，要求高部署率来保证成功率，更为重要的是标识信息泄露了 AS 间机密的商业关系和路由策略.

4.2 异常检测

异常检测的研究目标是有效识别前缀劫持、路径伪造和路由泄露等异常路由通告攻击，以帮助网络管理员深入了解互联网中 BGP 安全问题的真实状态，并且快速响应异常路由通告攻击，以降低攻击对域间路由系统的破坏，因此也是 BGP 安全研究的另一个主要方向.

如图 2 所示，目前 BGP 异常检测的研究内容主要包括异常检测技术、主动响应技术、异常检测系统和 BGP 可视化工具. 根据通用入侵检测系统框架(Common Intrusion Detection Framework，CIDF)[105]，响应单元是入侵检测系统的重要组成部分，在检测出异常事件后，只有快速、及时地响应，才能有效降低攻击造成的危害，达到保护系统的目的. 因此，本文将主动响应技术放到 BGP 异常检测研究方向中. 另外，BGP 可视化工具可使管理员形象地感知、分析和理解 BGP 路由变化，并发现异常事件，从而，该研究也是 BGP 异常检测的一个关键研究点.

4.2.1 异常检测技术

4.2.1.1 前缀劫持检测

异常检测技术的核心是对攻击特征的提取. 根据前缀劫持在控制、数据和管理平面的不同攻击特征，前缀劫持检测技术可分为以下几类.

(1)控制平面检测技术

前缀劫持在控制平面的特征是存在发生 MOAS 和 subMOAS 冲突的 short-lived 路由通告. 其中，MOAS(Multi-Origin AS，多源 AS)指某前缀存在多个源 AS，subMOAS 指前缀与其 more specific 前缀存在不同的源 AS. 前缀劫持控制平面检测技术的难点在于如何合理设置异常 MOAS 和 subMOAS 路由通告的生命期阈值. 常用方法是根据互联网中真实路由通告生命期的分布来设置该阈值[29-34].

(2)数据平面检测技术

前缀劫持在数据平面的特征是一些以被劫持前缀为目的地的数据流会被重定向到劫持网络，若劫持网络丢弃这些流量，将形成流量黑洞，导致受害网络不可达. 从而，前缀劫持数据平面检测技术要解决的关键问题是如何判断一些到达被劫持前缀的数据流被重定向. 解决方法包括：

① 探测受害网络的可达性状态

iSPY[35]中前缀拥有者采用 Traceroute 主动、持续地探测到达 3000 个 transit ASes 的可达性，若切断路径超过门限值，则认为本网络的前缀被劫持；Argus[36]使用 ping 命令在几分钟内并行、持续地探测到可疑前缀某 more specific 前缀的可达性，若该可疑前缀被劫持形成流量黑洞，则受污染网络向受害网络的数据平面探测将无法得到应答，反之可以. 因获取的信息有限，这类方法只能检测出会导致流量黑洞的前缀劫持.

② 探测、发现被劫持数据流的目的地、传输路径或传输特征等是否发生冲突或变化

文献[37]指出数据流重定向会导致使用被劫持前缀内 IP 地址的主机的数据平面指纹(如 Host OS 属性、IP ID、TCP timestamp、ICMP timestamp 等)发生冲突；文献[38]通过扫描 Internet 获得 SSL/TLS 数据来确认 subMOAS 事件中主机的公/私钥是否保持相同来排除恶意攻击；文献[39]观察到在数据流被重定向后从观测点到达被劫持前缀的网络距离(即跳数)会发生变化，且从观测点到被劫持前缀及其参考点前缀的路径会不一致；为了防止攻击者通过同时劫持参考点前缀来绕过上述检测机制，Buddyguard[40]进一步提出构建被劫持前缀的参考点前缀集合(称为 buddy 前缀)，若超过一定阈值的 buddy 前缀和被劫持前缀的路径不一致，则发生前缀劫持；LDC[41]提出通过被动监测前缀拥有者直接提供商的流量负载分布变化来识别前缀劫持的方法.

(3)管理平面检测技术

根据 RIR 或 IRR(Internet Routing Registries，Internet 路由注册机构)中记录，如果路由通告中的前缀和源 AS 不属于同一个组织[42-43]或所属组织不位于同一个区域(如国家或 RIRs)[44]，则认为发生前缀劫持攻击.

前缀劫持管理平面检测技术面临的挑战是 RIR 或 IRR 中注册数据是否真实且得到及时更新，有研究在实际分析真实的注册数据后，认为这些数据在某些情况下是真实可信的[106].

(4)进一步提高准确率的检测技术

① 多平面检测技术

受限于观测点的位置[107]，RouteViews、RIPE 等公开路由数据集中路由数据的真实性[108]和发生 MOAS、subMOAS 冲突的合法操作实践[32]，控制平面检测技术存在误报率和漏报率较高的问题. 对于数据平面探测技术，探测时机的选择是一个难点，如果持续不停探测会增加检测开销，仅在发现可疑事件后再进行探测是一个合理的作法. 因此，为了降低检测误报、漏报率和检测的开销，综合根据控制平面、数据平面和/或管理平面信息实施前缀劫持检测是一个有效方法. 目前通用作法[37-38]是首先根据控制平面信息发现 MOAS/subMOAS 事件，然后依次根据其它平面的信息过滤掉其中的合法事件或识别出其中的异常事件. 需要指出的是 Argus[36]首次通过计算控制平面结果和数据平面结果的关联系数，紧密结合控制和数据平面的检测结果实施判决，具有较高的准确度.

② 前缀拥有者检测技术

有些研究[31,43,45-46]认为只有前缀的拥有者才能够准确区分合法 MOAS 和前缀劫持事件，且拥有者能够快速采取措施来缓解、降低攻击造成的影响. 因此，为了提高检测准确度，可在发现可疑事件后，将其告知给前缀的真实拥有者，由其来判决. 该技术需要提前获知前缀的真实拥有者，且在发生前缀劫持，到被劫持前缀的数据流可能被重定向的情况下，如何将告知消息发送给前缀拥有者是必须解决的一个难点问题. PHAS[31]通过前缀拥有者注册，利用已有 e-mail 基础设施的多路径分发机制来实现消息告知；文献[45]要求 AS 在检测出路由通告的 MOAS 冲突后，将冲突路由通告转发给自己正在使用的该前缀的源 AS，而互联网 AS 拓扑的高度连接特性使阻塞由合法源 AS 发起的所有路由通告是非常困难的，从而可保证该前缀的真实拥有者能够获知冲突消息. 而且，为了避免前缀真实拥有者被大量无效告知消息淹没，该技术必须能够排除掉大量潜在合法的 MOAS 事件. 因 more specific 前缀劫持者会吸引互联网中几乎所有到达被劫持前缀的数据流，所以这种检测技术并不适用于检测 more specific 前缀劫持.

③ 协作检测技术

ASes 间协作检测也是提高检测准确率的方法之一. 如文献[42]提出邻居守望的方法，ASes 组成信任组，彼此交换信息和查寻异常行为；Co-Monitor[43]提出协作监测的思想，每个参与者与其它参与者交换彼此的前缀-源 AS 映射信息，并基于该信息实时监测本地路由更新，一旦发现不一致，则通知相关参与者；文献[47]将众包思想引入异常检测，提出参与者被动监控、彼此共享可疑信息、协作统计挖掘异常的方法.

上述典型前缀劫持检测技术的详细比较如表 4 所示.

表 4　典型前缀劫持检测技术比较

	检测类型							数据源					判决		系统架构		实时性
	regular 前缀劫持	more specific 前缀劫持	路径伪造	路由泄露	流量黑洞	流量窃听	流量欺诈	控制平面	数据平面	管理平面	前缀拥有者	协同检测	检测系统	拥有者	分布式	集中式	
PHAS	√	√	—	—	—	—	—	√	—	—	—	—	—	√	—	√	√
iSPY	√	—	—	—	—	—	—	—	√	—	—	—	—	√	√	—	√
文献[42]	√	√	—	—	—	—	—	—	—	√	—	√	√	—	√	√	—
文献[43]	√	√	—	—	—	—	—	—	—	—	√	√	—	√	√	—	√
文献[44]	√	√	—	—	—	—	—	—	—	√	—	—	√	—	—	√	—
文献[29,30]	√	√	—	—	—	—	—	√	—	—	—	—	√	—	—	√	—
文献[32]	√	—	—	—	—	—	—	√	—	—	—	—	√	—	—	√	—
Argus	—	—	—	—	√	—	—	√	√	—	—	—	√	—	—	√	√
文献[37]	√	√	—	—	—	—	—	√	√	—	—	—	√	—	—	√	√
文献[38]	—	√	—	—	—	—	—	√	√	√	—	—	√	—	—	√	√
文献[39]	—	—	—	—	—	√	√	—	√	—	—	—	√	—	√	—	√
Buddyguard	√	—	—	—	—	√	√	√	—	—	—	—	√	—	√	—	—
LDC	√	√	—	—	—	—	—	—	√	—	—	—	√	—	√	—	—
文献[45]	√	√	—	—	—	—	—	√	—	—	—	—	—	√	√	—	√
文献[46]	√	—	—	—	—	—	—	√	√	√	—	—	—	√	—	√	—
文献[47]	—	—	—	—	—	√	√	—	√	—	—	√	√	—	√	—	—

4.2.1.2　路径伪造与路由泄露检测

为检测路径伪造攻击，文献[49]根据控制平面信息构建源 AS 的下一跳 ASes 集合，然后，数据平面探测到源 AS 的路径，如果经过两次下一跳 AS，则认为发生路径伪造攻击；Whisper[48]在路由通告中增加对 AS_PATH 的签名，通过比较两个到达相

同目的地的路由通告的签名来验证这两个路径是否一致,若不一致,则触发报警;文献[36,50-51]根据网络拓扑中 AS 的位置(如核心或边缘)、AS 连接的流行度(即该 AS 连接在所有路由通告中出现的次数)和地理信息(如地理距离或地理偏航)等来识别伪造路径.

路由泄露的通用检测方法是根据推导出的 AS 间关系实施检测①.但是,受限于观测点的位置,根据路由数据推导出的 AS 间关系一般具有局限性.例如,文献[109]指出仅在一个大型 IXP 内检测出的 peer-peer 连接数目就相当于目前推导出的整个 Internet中 peer-peer 连接数目.又因为 AS 间关系和配置策略的复杂性[70,110],所以这类检测方法面临较高的漏报和误报挑战.

为降低误报率,文献[52]在基于 AS 间关系识别出 valley 路径的基础上,增加了 short-lived 和并发性特征,即作者认为被大量路由并发使用的 short-lived valley 路径就是被泄露的路由.有些研究根据因 AS 间关系导致的合法 AS 路径的独特特征实施检测.例如,文献[53]提出如果路由中含有两个非邻接 Tier-1 ASes,那么该路由是泄露路由,且泄露 AS 是路径中两个非邻接 Tier-1 ASes 间度数最低的 AS;文献[54]提出在初始已知 valley-free 路径的前提下,在 AS 不能与其提供商的提供商建立 peer 连接和 ASes 间不存在提供商关系循环连接的假设下,AS 能够根据自己的 RIB,识别出从 peer 或 customer 连接上收到的泄露路由,从而在路由泄露发起(Route Leak Initiation)[111]时就实施检测.

路径伪造和路由泄露也会导致流量重定向,因此一些数据平面探测技术(如文献[36,39,41,47])也可用于检测路径伪造和路由泄露攻击.

4.2.2 主动响应技术

目前 BGP 异常检测技术的研究成果对网络管理员发现、分析异常路由通告攻击起到了积极作用,但是要降低攻击造成的影响,真正保障 BGP 安全,仅靠检测技术是不够的,还需要主动响应技术研究的跟进.

对前缀劫持攻击而言,目前常用的响应方法是在检测出攻击后,首先通知真实源 AS 的管理员,由其配置、通告被劫持前缀的 more specific 前缀,然后,联系攻击者或攻击者的 ISPs 以停止非法的路由通告和传播.但是这种响应方法是一种被动响应,需要管理员的参与,且响应时间长.例如,2008 年的 Pakistan telecom hijack YouTube 事件中,从真实 YouTube 采取动作到恢复全网连接的 40%就花费了近 4 h.

鉴于此,有研究提出了对异常路由通告攻击的主动响应技术,以实现对攻击的主动、及时响应,有效降低攻击造成的危害.

在识别、发现可疑路由之后,PGBGP[33-34]将延迟可疑路由的使用和传播 T_s 时间(通常设置为 1 天).在可疑期 T_s 内,PGBGP 路由器使用替代路径来转发数据;如果可疑路由是真实攻击,在 T_s 内其可能已被真实源 AS 撤销,如果 T_s 后,可疑路由仍然存在,路由器则认为该路由是合法的.在 PGBGP 中,路由传播在每跳都被延迟 T_s 时间,将延长所有可疑但合法路由的收敛时间.不同于 PGBGP,在识别、发现可疑路由后,QBGP[55]在可疑期内解耦合路径传播和数据转发,即路由器使用可信的替代路径来转发数据,以保护数据流,但是仍然向邻居传播此可疑路由,以使异常检测系统能够快速发现攻击.为了标识可疑路由,QBGP 需要修改 BGP 协议,引入新的路径属性 QASPATH 与 PGBGP 和 QBGP 不同,PurgePromote[56]本身不识别可疑路由,而是根据异常检测系统的实时检测结果(攻击 AS、受害 AS 和被劫持前缀),识别出伪造路由和有效路由,然后通知网络中的 lifesaver AS 删除(purge)路由表中的伪造路由,promoter AS 提升(promote)有效路由,promoter AS 提升路由的方法是将有效路由 AS_PATH 中的路径设置为 AS_SET,从而缩短 AS_PATH 长度.PurgePromote 不破坏路由系统的收敛性,且实现了对检测结果的主动、及时响应,有效缓解了攻击造成的危害.

4.2.3 异常检测系统

根据采用的系统架构,异常检测系统可分为集中式和分布式两类.BGPMon②、Team Cymru③是典型的集中式检测系统,它们集中从分布式监测器中收集路由数据,创建关于路由异常的警报/总结报告,并通知相应的注册组织.集中式检测系统 BGP-MAS[57]监控进入路由器的路由通告,若发现异常通告,则发出声音报警,且向 AS 管理员显示异常通告的来源.

因恶意攻击经常覆盖多个域,不再是孤立事件,所以单个网络实体的检测变得困难[112].网络实体

① BGP Routing Leak Detection System. http://puck.nether.net/bgp/leakinfo.cgi, 2016.5.11
② BGPmon. http://www.bgpmon.net/, 2016.5.16
③ Team Cymru. http://www.team-cymru.org, 2016.5.16

的联合可提供更加丰富的信息，有助于识别、检测这种大规模攻击. 分布式合作系统 PrefiSec[58] 提供了可扩展的、完全分布式的架构实现信息共享，通过有效聚合证据信息实现对大规模攻击的通知告警. 协同审计系统 NetReview[59] 要求每个路由器以一种 tamper-evident log 形式记录其发送或接收的 BGP 路由报文，且提出了一种规则描述语言，以描述最优实践、路由规则等，ASes 通过审计日志是否遵守这些规则来检测故障. BGPInspector[60] 提出了一个易于扩展的 Internet 监控框架，通过集成已有前缀级监控器 Buddyguard[40] 和全球级监控器 I-seismograph[113]，实现对域间路由系统的并行、实时和多粒度监测.

4.2.4　BGP 可视化工具

BGP 可视化工具可帮助管理员形象地感知、分析和理解 BGP 路由变化，并发现异常[114-115]. 根据视图显示的粒度，BGP 可视化工具可分为 3 类：(1) AS 粒度视图. BGPlay①、LinkRank[61] 和 TAMP[62] 根据原始的 BGP 更新报文，实现 AS 级别 BGP 路由变化的动画显示；VAST[63] 实现了互联网 AS 级网络拓扑的 3D 显示；Cyclops[64] 通过显示某特定 ISP 的 AS 级连接视图，帮助该 ISP 管理员检测和诊断本网络的路由异常；(2) IP 粒度视图. BGPeep[65] 从 IP 地址空间的角度实现 BGP 路由变化的动画显示；ELISHA[66-67] 采用像素显示的方法实现 MOAS 事件的 3D 显示，并且根据不同的 MOAS 事件类型进行着色区分，通过捕捉视图中的颜色异常来发觉异常 MOAS 事件；(3) 多粒度视图. BGP Eye[68] 提供了实时路由状态的 Internet-Centric 和 Home-Centric 视图，以及对 BGP 事件的各种统计分析数据，如某 AS 链路上的 BGP 事件数、前缀状态和稳定性等，来帮助管理员分析造成路由中断的根本原因；VisTracer[69] 综合采用像素、图像字符、时态图像等显示技术实现对异常检测结果(如异常事件类型、过程、相关 AS、前缀变化等)的视图化综合显示，以帮助分析员探索、识别和分析可疑事件与恶意行为之间的关联.

5　研究挑战与展望

5.1　安全防护

(1) 安全防护技术应满足的要求

RPKI 和 ROA 技术可有效解决前缀劫持攻击问题，但是却面临 RPKI 全网部署的最大挑战. 部署 RPKI 意味着 ISPs 在入网前首先要到国际地址分配机构申请相关网络资源(如 IP 地址、AS 号码)的资源证书，获得“入网许可”. 这种“集中权威式”管理与互联网、域间路由系统的开放、分布、自治本质相违背，会引发互联网管理权之争[116]. 所以，目前 RPKI 的部署变成了互联网中成千上万自治 ISPs 间的协商游戏. 而且，有学者研究发现仅局部部署实现 RPKI时，只能得到有限的安全保障[117-118]，且会引入新的不稳定和安全问题[84,119]. 另外，虽然 BGPsec 技术从理论上可有效解决路径伪造攻击问题，但是也面临着计算、存储开销大，修改路由协议，需升级路由器硬、软件等部署挑战[120]，所以还未形成标准草案[121]. 轻量级 ROVER 方案得到研究人员的推崇，但是其只能解决前缀劫持攻击问题，而且未来部署前景不明朗. 因泄露了 AS 间机密的商业关系和路由策略，目前仍然没有有效的路由泄露防护方法[75].

通过上述分析，我们认为有效的 BGP 安全防护技术应满足以下要求：

①尽可能地不修改路由协议、路由器；

②尽可能地不增加路由器计算、存储等开销，如采用外包实现；

③与域间路由系统开放、分布、自治和商业性的特性相契合.

(2) RPKI 相关研究

RPKI 是保障 BGP 安全的重要支撑性基础设施. 目前 RPKI 主要技术原理已经较清晰，下步主要研究内容包括由权力“集中”的 RPKI 权威带来的安全问题、RPKI 实现、部署困境分析与解决[122-123]、部署测量和监测工具等，以促进 RPKI 的实现和部署.

(3) 轻量级路径认证研究

目前 BGP 路径认证技术需要修改 BGP 协议、增加了路由器的存储和处理开销，难以部署实现. 轻量级路径认证技术的研究将是未来研究的一个重要方向，也是一个难点[124].

(4) 安全外包技术研究

不修改路由协议，不增加路由器负担，与 BGP 路由解耦合，外包解决 BGP 安全问题是一个很有价值的研究方向.

(5) 路由泄露防护技术研究

鉴于 AS 间商业关系的机密性和复杂性，路由

① BGPlay. https://stat.ripe.net/special/bgplay#carousel, 2016.5.10

泄露的安全防护具有很大的挑战性.路由泄露防护技术要解决好信息告知与信息泄露之间的矛盾,即在向邻居传播路由通告时,为防止路由泄露的发生,需要告知邻居某些信息,如对该路由通告的许可操作(如允许向客户传播等),而该信息却会导致 AS 间机密的商业关系的泄露.

5.2 异常检测

(1)前缀劫持、路径伪造检测技术研究

目前 BGP 异常检测技术能够识别出前缀劫持、路径伪造攻击,但是面临着检测误报和漏报率高的问题.如何在目前研究基础上进一步降低检测的误报和漏报率是需要深入研究的一个难点问题.对控制平面、数据平面和管理平面的检测结果开展数学分析和关联可能是解决该问题的一个突破口.另外,攻击者有可能通过巧妙地设计攻击步骤来绕过检测系统,因此,如何避免攻击者规避检测也是检测技术研究时需要考虑的内容.而且,异常检测系统还应该提供详细的检测结果,包括攻击 AS、被劫持前缀、受害 AS 等,以有助于对攻击的主动响应和事后追责.

(2)路由泄露检测技术研究

因路由泄露"路由信息真实,路由传播非法"的特殊性,在 AS 间商业关系机密的前提下,路由泄露的识别、检测是一个难点问题.深入挖掘、分析路由泄露在控制平面、数据平面所表现出的攻击特征,或泄露路径特征,将有助于该问题的解决.

(3)主动响应技术研究

对攻击检测结果实施主动响应才能够及时、有效的缓解攻击造成的危害.因此,异常路由通告攻击的主动响应技术是未来需要深入研究的一个方向.

5.3 域间路由信任

在解决 BGP 安全问题时,有些研究人员尝试引入了信任技术.如文献[125]提出基于网络管理员间的信任关系来构建一个覆盖网络,通过彼此之间共享路由、前缀等信息来实现对前缀劫持、路径伪造等攻击的检测;文献[126]提出 AS-CRED 机制,通过评估自治系统发起前缀可达路由通告的信誉,来降低前缀劫持攻击检测的误报率;为提供互联网域间路由状态的全局视图,文献[127]提出 AS-TRUST 机制,以刻画自治系统通告有效(准确、稳定、符合路由策略)路由的全局信誉;文献[128]提出一个 AS 信誉系统 ASwatch,通过监控 AS 的控制平面行为来识别恶意 AS.

文献[129-131]提出了一种域间路由信任技术.该技术的主要思想是评估自治系统的域间路由行为,以构建该系统的域间路由信任度,从而在选择最优路由时,优选由高可信自治系统通告/传播的路由,过滤由低可信自治系统通告的路由.最终,实现对前缀劫持、路径伪造和路由泄露等异常路由通告攻击的有效抑制.

本文认为域间路由信任技术为解决 BGP 安全问题提供了一条除安全防护、异常检测外的可行途径.首先,域间路由信任技术不是通过弥补 BGP 的安全缺陷来保障 BGP 安全,而是通过抑制攻击的发生来改善 BGP 安全,实现的是一种"软安全";其次,该技术与域间路由系统分布、自治的本质相契合,可采用与域间路由系统解耦合、外包的方法实现,是一种轻量级解决方案,具有良好的可实施性;第三,域间路由信任技术还可激励合法自治系统,惩罚进行攻击行为的恶意自治系统,有助于域间路由系统整体安全性的改善和提高;最后,域间路由系统满足交互信任的建立条件,包括自治系统长期稳定存在,自治系统的域间路由行为"理性"、具有一定的连续性和社会行为特征等.

但是,目前域间路由信任技术只是 P2P、ad hoc 等领域信任技术研究成果[132-134]在域间路由系统中的应用,忽略了域间路由系统与 P2P、ad hoc 等系统在系统规模、行为特征与动态性、自治系统间关系等方面的差异性.因此,有必要对域间路由信任技术的一些基础理论问题展开探索研究,包括面对自治系统发起和传播路由通告两种不同域间路由行为,采用一个信任值度量是否合适?仅基于异常检测结果评估域间路由行为是否恰当?域间路由信任度的计算方法是否适用于具有大规模、分布、自治和商业性特性的域间路由系统?域间路由信任度的动态演化方法是否能够实现信任的快速收敛?等问题.

5.4 域间路由系统测量

随着互联网规模的日益扩大和域间路由系统的日益复杂,对域间路由系统的测量将有助于 BGP 安全的解决.如文献[135]对互联网路由策略的调查研究发现有 87% 网络遵循 LP 最优路由选择策略,68% 遵循 LP 最优路由选择和 GR 路由出站策略,在选择最优路径时仅有 9% 网络将安全置于最优路径选择策略的第 1 位,40% 网络将安全置于 SP 策略之后.该发现对于 BGP 安全方案,特别是路由泄露相关安全方案的设计和策略配置有重要的指导作用.文献[109]发现由 RouteViews 和 RIPE RIS 提供的公开 BGP 数据集中存在伪造路由.该发现将对目前异常路由通告控制平面检测技术的准确度产生一

定影响.安全学者一般都认为 IRR 注册信息不准确和不及时，不能用于检测前缀劫持，但是文献[107]却调查发现互联网中 82%的 ASes，特别是中小型 transit 提供商(customer zones<1000)，在 IRR 中真实注册了自己的前缀信息.因此，有针对性地开展对实际域间路由系统的拓扑结构、发起和传播路由行为特征及其动态性、路由策略、注册和路由数据的真实性及覆盖度等方面的测量研究，将有助于安全人员理解域间路由系统及其实际特性，以更有效地设计、实现 BGP 安全解决方案.

6 总　结

BGP 安全是网络安全领域的一个重要研究方向.本文在清晰刻画 BGP 安全威胁模型的基础上，从安全防护和异常检测两个方面，对近年来 BGP 安全技术的研究现状进行了详细的分类阐述、总结、归纳和分析比较，最后，探讨、展望了该领域研究的难点问题和需进一步研究的内容.本文针对 BGP 安全的综述研究希望能够为相关研究人员和网络安全专家提供借鉴和帮助.

参　考　文　献

[1] Murphy S. BGP security vulnerabilities analysis. RFC 4272, 2006

[2] Li Song, Zhuge Jian-Wei, Li Xing. Study on BGP security. Journal of Software, 2013, 24(1): 121-138(in Chinese)
(黎松，诸葛建伟，李星. BGP 安全研究. 软件学报，2013, 24(1): 121-138)

[3] Nordstrom O, Dovrolis C. Beware of BGP attack. ACM Computer Communications Review, 2004, 34(2): 1-8

[4] Huston G, Rossi M, Armitage G. Securing BGP—A literature survey. IEEE Communications Surveys & Tutorials, 2011, 13(2): 199-222

[5] Butler K, Farley TR, MaDaniel P, Rexford J. A survey of BGP security issues and solutions. Proceedings of the IEEE, 2010, 98(1): 100-122

[6] Vervier P-A, Thonnard O, Dacier M. Mind your blocks: On the stealthiness of malicious BGP hijacks//Proceedings of the 2015 Network and Distributed System Security (NDSS) Symposium. San Diego, USA, 2015: 8-11

[7] Goldberg S. Why is it taking so long to secure internet routing? Communications of the ACM: ACM Queue, 2014, 57(10): 56-63

[8] Hu Y-C, Perrig A, Sirbu M. SPV: Secure path vector routing for securing BGP. ACM Computer Communication Review, 2004, 34(4): 179-192

[9] Zhao M, Smith W S, Nicol M D. Aggregated path authentication for efficient BGP security//Proceedings of the 12th ACM Conference on Computer and Communications Security (CCS 2005). Alexandria, USA, 2005: 128-138

[10] Li Qi, Wu Jian-Ping, Xu Ming-Wei, et al. GesBGP: A good-enough-security BGP. Chinese Journal of Computers, 2009, 32(3): 506-515(in Chinese)
(李琦，吴建平，徐明伟等. 自治系统间的安全路由协议 GesBGP. 计算机学报，2009, 32(3): 506-515)

[11] Wang Na, Zhi Ying-Jian, Zhang Jian-Hui, et al. Identity-based secure inter-domain routing protocol. Journal of Software, 2009, 20(12): 3223-3239(in Chinese)
(王娜，智英建，张建辉等. 一个基于身份的安全域间路由协议. 软件学报，2009, 20(12): 3223-3239)

[12] Chen P, Wang X, Wu Y, et al. iPKI: Identity-based private key infrastructure for securing BGP protocol//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security. Denver, USA, 2015: 1632-1634

[13] Li Dao-Feng, Wang Gao-Cai, Wang Zhi-Wei, et al. Provable secure mechanism for BGP path protection in the standard model. Chinese Journal of Computers, 2015, 38(4): 859-871(in Chinese)
(李道丰，王高才，王志伟等. 标准模型下可证明安全的 BGP 路由属性保护机制. 计算机学报，2015, 38(4): 859-871)

[14] White R. Securing BGP through secure origin BGP (soBGP). The Internet Protocol Journal, 2003, 6(3): 15-22

[15] van Oorschot P C, Wan T, Kranakis E. On interdomain routing security and pretty secure BGP (psBGP). ACM Transactions on Information and System Security, 2007, 10(3): 11-46

[16] Hu Xiang-Jiang, Zhu Pei-Dong, Gong Zheng-Hu. SE-BGP: An approach for BGP security. Journal of Software, 2008, 9(1): 167-176(in Chinese)
(胡湘江，朱培栋，龚正虎. SE-BGP：一种 BGP 安全机制. 软件学报，2008, 9(1): 167-176)

[17] Butler K, McDaniel P, Aiello W. Optimizing BGP security by exploiting path stability//Proceedings of the 13th ACM Conference on Computer and Communications Security. Alexandria, USA, 2006: 298-310

[18] Yang X, Xingang S, Jianping W, et al. Sign what you really care about—Secure BGP AS-paths efficiently. Computer Networks, 2013, 57(10): 2250-2265

[19] Aiello W, Ioannidis J, McDaniel P. Origin authentication in interdomain routing//Proceedings of the 10th ACM Conference on Computer and Communications Security. Washington, USA, 2003: 165-178

[20] Lepinski M, Kent S. An infrastructure to support secure Internet routing. RFC 6480, 2012

[21] Huston G, Michaelson G. Validation of route origination using the resource certificate Public Key Infrastructure (PKI) and Route Origin Authorizations (ROAs). RFC 6483, 2012

[22] Lepinski M, Sriram K. BGPsec protocol specification. draft-ietf-sidr-bgpsec-protocol-15, 2016

[23] Goodell G, Aiello W, Griffin T, et al. Working around BGP: An incremental approach to improving security and accuracy in interdomain routing//Proceedings of the 2003 Internet Society Symposium on Network and Distributed System Security (NDSS'03). San Diego, USA, 2003: 75-85

[24] Gersch J, Massey D. ROVER: Route origin verification using DNS//Proceedings of the 2013 22nd International Conference on Computer Communications and Networks (ICCCN). Nassau, Bahamas, 2013: 1-9

[25] Sundaresan S, Lychev R, Valancius V. Preventing attacks on BGP policies: One bit is enough. Technical Report GT-CS-11-07, Georgia Institute of Technology, Atlanta, USA, 2011

[26] Qiu S Y, McDaniel P D, Monrose F. Toward valley-free interdomain routing//Proceedings of the 2007 IEEE International Conference on Communications. Glasgow, Scotland, 2007: 2009-2016

[27] Dickson B. Route leaks -requirments for detection and prevention thereof. draft-dickson-sidr-route-leak-reqts-02, 2012

[28] Sriram K, Montgomery D, Dickson B, et al. Methods for detection and mitigation of BGP route leaks. draft-ietf-idr-route-leak-detection-mitigation-02, 2015

[29] Boothe P, Hiebert J, Bush R. How Prevalent is prefix hijacking on the Internet. NANOG36 Talk, 2006

[30] Khare V, Ju Q, Zhang B. Concurrent prefix hijacks: Occurrence and impacts//Proceedings of the 2012 ACM Conference on Internet Measurement Conference. Boston, USA, 2012: 29-36

[31] Lad M, Massey D, Pei D, et al. PHAS: A prefix hijack alert system//Proceedings of the 15th Conference on USENIX Security Symposium—Volume 15. Vancouver, Canada, 2006: 153-166

[32] Zhao X, Pei D, Wang L, et al. An analysis of BGP multiple origin AS (MOAS) conflicts//Proceedings of the 1st ACM SIGCOMM Workshop on Internet Measurement. San Francisco, USA, 2001: 31-35

[33] Karlin J, Forrest S, Rexford J. Autonomous security for autonomous systems. ACM Computer Communication Review, 2008, 52(15): 2908-2923

[34] Karlin J, Forrest S, Rexford J. Pretty good BGP: Improving BGP by cautiously adopting routes//Proceedings of the IEEE International Conference on Network Protocols. Santa Barbara, USA, 2006: 290-299

[35] Zhang Z, Zhang Y, Hu Y C, et al. iSPY: Detecting IP prefix hijacking on my own. IEEE/ACM Transactions on Networking, 2010, 18(6): 1815-1828

[36] Xingang S, Yang X, Zhiliang W, et al. Detecting prefix hijackings in the Internet with Argus//Proceedings of the 2012 ACM Conference on Internet Measurement Conference (IMC'12). Boston, USA, 2012: 15-28

[37] Hu X, Mao Z M. Accurate real-time identification of ip prefix hijacking//Proceedings of the IEEE Symposium on Security and Privacy. Berkeley, USA, 2007: 3-17

[38] Schlamp J, Holz R, Gasser O, et al. Investigating the nature of routing anomalies: Closing in on subprefix hijacking attacks//Proceedings of the 7th International Workshop on Traffic Monitoring and Analysis (TMA 2015). Barcelona, Spain, 2015: 173-187

[39] Zheng C, Ji L, Pei D, et al. A light-weight distributed scheme for detecting ip prefix hijacks in real-time. ACM Computer Communication Review, 2007, 37(4): 277-288

[40] Li J, Ehrenkranz T, Elliott P. Buddyguard: A buddy system for fast and reliable detection of IP prefix anomalies//Proceedings of the 2012 20th IEEE International Conference on Network Protocols (ICNP). Austin, USA, 2012: 1-10

[41] Liu Y, Su J, Chang R K C. LDC: Detecting BGP prefix hijacking by load distribution change//Proceedings of the 2012 IEEE 26th International Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW). Shanghai, China, 2012: 1197-1203

[42] Signanos G, Faloutsos M. Neighborhood watch for Internet routing: Can we improve the robustness of Internet routing today?//Proceedings of the IEEE INFOCOM 2007. Washington, USA, 2007: 1271-1279

[43] Liu Xin, Zhu Pei-Dong, Peng Yu-Xing. Co-Monitor: Collaborative monitoring mechanism for detecting prefix hijacks. Journal of Software, 2010, 21(10): 2584-2598(in Chinese) (刘欣, 朱培栋, 彭宇行. Co-Monitor: 检测前缀劫持的协作监测机制. 软件学报, 2010, 21(10): 2584-2598)

[44] Sanchez F, Duan Z. Region-based BGP announcement filtering for improved BGP security//Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security. Beijing, China, 2010: 89-100

[45] Qiu S, Monrose F, Terzis A, McDaniel P. Efficient techniques for detecting false origin advertisements in inter-domain routing//Proceedings of the 2006 2nd IEEE Workshop on Secure Network Protocols. Santa Barbara, USA, 2006: 12-19

[46] Vervier P A, Jacquemart Q, Schlamp J, et al. Malicious BGP hijacks: Appearances can be deceiving//Proceedings of the 2014 IEEE International Conference on Communications (ICC). Sydney, Australia, 2014: 884-889

[47] Hiran R, Carlsson N, Shahmehri N. Crowd-based detection of routing anomalies on the internet//Proceedings of the 2015 IEEE Conference on Communications and Network Security (CNS). San Francisco, USA, 2015: 388-396

[48] Lakshminarayanan S, Volker R, Ion S, et al. Listen and whisper: Security mechanisms for BGP//Proceedings of the 1st Conference on Symposium on Networked Systems Design and Implementation—Volume 1. San Francisco, USA, 2004: 10-24

[49] Ballani H, Francis P, Zhang X. A study of prefix hijacking and interception in the internet. ACM SIGCOMM Computer Communication Review, 2007, 37(4): 265-276

[50] Theodoridis G, Tsigkas O, Tzovaras D. A novel unsupervised method for securing BGP against routing hijacks//Proceedings of the 27th International Symposium on Computer and Information Sciences. Paris, France, 2012: 21-29

[51] Kruegel C, Mutz D, Robertson W, Valeur F. Topology-based detection of anomalous BGP messages//Proceedings of the 6th International Symposium on Recent Advances in Intrusion Detection. Berlin, Germany, 2003: 17-35

[52] Shen S, Beichuan Z, Lin Y, et al. Towards real-time route leak events detection//Proceedings of the 2015 IEEE International Conference on Communications (ICC). London, UK, 2015: 7192-7197

[53] Li S, Duan H, Wang Z, Li X. Route leaks identification by detecting routing loops//Proceedings of the 11th International Conference on Security and Privacy in Communication Networks. Dallas, USA, 2015: 313-329

[54] Siddiqui M S, Montero D, Serral-Gracia R, Yannuzzi M. Self-reliant detection of route leaks in inter-domain routing. The International Journal of Computer and Telecommunications Networking, 2015, 82(C): 135-155

[55] Mingui Z, Bin L, Beichuan Z. Safeguarding data delivery by decoupling path propagation and adoption//Proceedings of the IEEE INFOCOM 2010. San Diego, USA, 2010: 1-5

[56] Zhang Z, Zhang Y, Hu Y C, Mao Z M. Practical defenses against BGP prefix hijacking//Proceedings of the 2007 ACM CoNEXT Conference. New York, USA, 2007: 1-12

[57] Yun J-K, Hong B, Kim Y. The BGP monitoring and alarming system to detect and prevent anomaly IP prefix advertisement//Proceedings of the 2013 Research in Adaptive and Convergent Systems. Montreal, Canada, 2013: 232-236

[58] Hiran R, Carlsson N, Shahmehri N. PrefiSec: A distributed alliance framework for collaborative BGP monitoring and prefix-based security//Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security. Scottsdale, USA, 2014: 3-12

[59] Haeberlen A, Avramopoulos I, Rexford J, Druschel P. NetReview: Detecting when interdomain routing goes wrong//Proceedings of the 6th USENIX Symposium on Networked Systems Design and Implementation. Boston, USA, 2009: 437-452

[60] Mingui Z. BGPInspector: A real-time extensible Border Gateway Protocol monitoring framework. Technical Report DRP-201411, University of Oregon, Eugene, USA, 2014

[61] Lad M, Massey D, Zhang L. Visualizing Internet routing changes. IEEE Transactions on Visualization and Computer Graphics, 2006, 12(6): 1450-1460

[62] Wong T, Van J, Alaettinoglu C. Internet routing anomaly detection and visualization//Proceedings of the 2005 International Conference on Dependable Systems and Networks (DSN'05). Yokohama, Japan, 2005: 172-181

[63] Oberheide J, Karir M, Blazakis D. VAST: Visualizing autonomous system topology//Proceedings of the 3rd International Workshop on Visualization for Computer Security. Alexandria, USA, 2006: 71-80

[64] Chi Y-J, Oliveira R, Zhang L. Cyclops: The AS-level connectivity observatory. ACM SIGCOMM Computer Communication Review, 2008, 38(5): 5-16

[65] Shearer J, Ma K-l, Kohlenberg T. BGPeep: An IP-space centered view for Internet routing data//Proceedings of the 5th International Workshop on Visualization for Computer Security. Cambridge, USA, 2008: 95-110

[66] Teoh S-T, Ma K-L, Wu S F, et al. Visual-based anomaly detection for BGP origin AS change (OASC) events//Proceedings of the 14th IFIP/IEEE International Workshop on Distributed Systems: Operations and Management (DSOM 2003). Berlin, Germany, 2003: 155-168

[67] Teoh S-T, Ma K-L, Wu S F, et al. Elisha: A visual-based anomaly detection system//Proceedings of the 5th International Symposium on Recent Advances in Intrusion Detection (RAID). Zurich, Switzerland, 2002

[68] Teoh S T, Ranjan S, Nucci A, Chuah C-N. BGP eye: A new visualization tool for real-time detection and analysis of BGP anomalies//Proceedings of the 3rd International Workshop on Visualization for Computer Security. Alexandria, USA, 2006: 81-90

[69] Fischer F, Fuchs J, Vervier P-A, et al. VisTracer: A visual analytics tool to investigate routing anomalies in traceroutes//Proceedings of the 9th International Symposium on Visualization for Cyber Security. Seattle, USA, 2012: 80-87

[70] Giotsas V, Luckie M, Huffaker B, Claffy K. Inferring complex AS relationships//Proceedings of the 2014 Conference on Internet Measurement Conference. Vancouver, Canada, 2014: 23-30

[71] Lixin G, Griffin T G, Rexford J. Inherently safe backup routing with BGP//Proceedings of the INFOCOM 2001 20th Annual Joint Conference of the IEEE Computer and Communications Societies. Anchorage, USA, 2001: 547-556

[72] Gao L, Rexford J. Stable Internet routing without global coordination. ACM Transactions on Networking, 2001, 9(6): 681-692

[73] Touch J, Mankin A, Bonica R. The TCP Authentication Option. RFC 5925, 2010

[74] Biersack E, Jacquemart Q, Fischer F, et al. Visual analytics for BGP monitoring and prefix hijacking identification. IEEE Network, 2012, 26(6): 33-39

[75] Sriram K, Montgomery D, McPherson D, et al. Problem definition and classification of BGP route leaks. draft-ietf-grow-route-leak-problem-definition-04. 2016

[76] Kent S, Lynn C, Seo K. Secure border gateway protocol (secure-BGP). IEEE Journal on Selected Areas in Communications, 2000, 18(4): 582-592

[77] Seberry J, Mu Y, Guo F, Wellsmore T. Efficient authentication and integrity protection for the border gateway protocol. International Journal of Security and Networks, 2014, 9(4): 234-243

[78] Cohen A, Gilad Y, Herzberg A, Schapira M. One hop for RPKI, one giant leap for BGP security//Proceedings of the 14th ACM Workshop on Hot Topics in Networks. Philadelphia, USA, 2015: 1-7

[79] Brogle K, Goldberg S, Reyzin L. Sequential aggregate signatures with lazy verification from trapdoor permutations. Information and Computation, 2014, 239(C): 356-376

[80] Raghavan B, Panjwani S, Mityagin A. Analysis of the SPV secure routing protocol: Weaknesses and lessons. ACM SIGCOMM Computer Communication Review, 2007, 37(2): 29-38

[81] Lepinski M, Kent S, Kong D. A profile for Route Origin Authorizations (ROAs). RFC 6482, 2012

[82] Bellovin S, Rush R, Ward D. Security requirements for BGP path validation. RFC 7353, 2014

[83] Kent S, Chi A. Threat model for BGP path security. RFC 7132, 2014

[84] Cooper D, Heilman E, Brogle K, et al. On the risk of misbehaving RPKI authorities//Proceedings of the 12th ACM Workshop on Hot Topics in Networks, College Park. Maryland, USA, 2013: 1-7

[85] Heilman E, Cooper D, Reyzin L, Goldberg S. From the consent of the routed: Improving the transparency of the RPKI// Proceedings of the 2014 ACM Conference on SIGCOMM. Chicago, USA, 2014: 51-62

[86] Kent S, Mandelberg D. Suspenders: A fail-safe mechanism for RPKI. draft-kent-sidr-suspenders-04, 2015

[87] Bush R. Responsible grandparenting in the RPKI. draft-ymbk-rpki-grandparenting-04, 2014

[88] Bush R. RPKI local trust anchor use cases. draft-ietf-sidr-lta-use-cases-04, 2013

[89] Wahlisch M, Holler F, Schmidt T C, Schiller J H. Updates from the Internet backbone: An RPKI/TRT router implementation, measurements, and analysis//Proceedings of the Network and Distributed System Security Symposium (NDSS) 2013. San Diego, USA, 2013: 1-11

[90] Wahlisch M, Schmidt T C. See how ISPs care: An RPKI validation extension for Web browsers. ACM SIGCOMM Computer Communication Review, 2015, 45(4): 115-116

[91] Iamartino D, Pelsser C, Bush R. Measuring BGP route origin registration and validation//Proceedings of the 16th International Conference on Passive and Active Measurement (PAM 2015). Berlin, Germany, 2015: 28-40

[92] Wahlisch M, Schmidt R, Schmidt T C, et al. RiPKI: The tragic story of RPKI deployment in the web ecosystem// Proceedings of the 14th ACM Workshop on Hot Topics in Networks. Philadelphia, USA, 2015: 1-7

[93] Osterweil E, McPherson D. Sizing estimates for a fully deployed RPKI. Technical Report 1120005, Verisign Labs, Reston, USA, 2012

[94] Wahlisch M, Maennel O, Schmidt T C. Towards detecting BGP route hijacking using the RPKI. ACM SIGCOMM Computer Communication Review, 2012, 42(4): 103-104

[95] Reuter A, Wahlisch M, Schmidt T C. RPKI MIRO: Monitoring and inspection of RPKI objects. ACM SIGCOMM Computer Communication Review, 2015, 45(4): 107-108

[96] Grimaldi G, Manto M. Internet security and networked governance in international relations. International Studies Review, 2013, 15(1): 86-104

[97] Kuerbis B, Mueller M L. Negotiating a new governance hierarchy: An analysis of the conflicting incentives to secure Internet routing. Communications and Strategies, 2011, (81): 125-142

[98] Na W, Yingjian Z, Binqiang W. AT: An origin verification mechanism based on assignment track for securing BGP// Proceedings of the IEEE International Conference on Communications, 2008. Beijing, China, 2008: 5739-5745

[99] Lu Xi-Cheng, Zhao Jin-Jing, Zhu Pei-Dong, Dong Pan. Self-organization of inter-domain routing system. Journal of Software, 2006, 17(9): 1922-1932(in Chinese)
(卢锡城, 赵金晶, 朱培栋, 董攀. 域间路由系统自组织特性. 软件学报, 2006, 17(9): 1922-1932)

[100] Piscitello D. Guidance for preparing domain name orders, seizures & takedowns. Technical Report, ICANN. March 2012

[101] Soghoian C, Stamm S. Certified lies: Detecting and defeating government interception attacks against SSL (Short Paper)// Proceedings of the 15th International Conference on Financial Cryptography and Data Security. Berlin, Germany, 2012: 250-259

[102] Malhotra A, Goldberg S. RPKI vs ROVER: Comparing the risks of BGP security solutions//Proceedings of the 2014 ACM Conference on SIGCOMM. Chicago, USA, 2014: 113-114

[103] McPherson D, Amante S, Osterweil E, Mitchell D. Route-leaks & MITM attacks against BGPSEC. draft-ietf-grow-simple-leak-attack-bgpsec-no-help-04, 2014

[104] Goldberg S, Schapira M, Hummon P, Rexford J. How secure are secure interdomain routing protocols. ACM Computer Communication Review, 2010, 40(4): 87-98

[105] Garcia-Teodoro P, Diaz-Verdejo J, Macia-Fernandez G, Vazquez E. Anomaly-based network intrusion detection: Techniques, systems and challenges. Computers and Security, 2009, 28(1-2): 18-28

[106] Khan A, Kim H-C, Kwon T, Choi Y. A comparative study on IP prefixes and their origin ases in BGP and the IRR. ACM SIGCOMM Computer Communication Review, 2013, 43(3): 16-24

[107] Zhang Y, Zhang Z, Mao Z M, et al. On the impact of route monitor selection//Proceedings of the 7th ACM SIGCOMM Conference on Internet Measurement. San Diego, USA, 2007: 215-220

[108] Luckie M. Spurious routes in public BGP data. ACM SIGCOMM Computer Communication Review, 2014, 44(3): 14-21

[109] Ager B, Chatzis N, Feldmann A, et al. Anatomy of a large European IXP//Proceedings of the ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication. Helsinki, Finland, 2012: 163-174

[110] Giotsas V, Zhou S. Valley-free violation in Internet routing analysis based on BGP community data//Proceedings of the 2012 IEEE International Conference on Communications (ICC). Ottawa, Canada, 2012: 1193-1197

[111] Dickson B. Route leaks—definitions. draft-dickson-sidr-route-leak- def-03, 2012

[112] Anirudh R, Nick F. Understanding the network-level behavior of spammers//Proceedings of the 2006 ACM Conference on SIGCOMM. Pisa, Italy, 2006: 291-302

[113] Li J, Brooks S. I-seismograph: Observing and measuring Internet earthquakes//Proceedings of the IEEE INFOCOM 2011. Shanghai, China, 2011: 2624-2632

[114] Biersack E, Jacquemart Q, Fischer F, et al. Visual analytics for BGP monitoring and prefix hijacking identification. IEEE Network, 2012, 26(6): 33-39

[115] Zhao Ying, Fan Xiao-Ping, Zhou Fang-Fang, et al. A survey on setwork security data visualization. Journal of Computer-Aided Design & Computer Graphics, 2014, 26(5): 687-697 (in Chinese)
(赵颖, 樊晓平, 周芳芳等. 网络安全数据可视化综述. 计算机辅助设计与图形学学报, 2014, 26(5): 687-697)

[116] Kuerbis B, Mueller M. Negotiating a new governance hierarchy: An analysis of the conflicting incentives to secure Internet routing. Communications and Strategies, 2011, 81(2011): 125-142

[117] Goldberg S, Schapira M, Hummon P, Rexford J. How secure are secure interdomain routing protocols? ACM SIGCOMM Computer Communication Review, 2010, 40(4): 87-98

[118] Lychev R, Goldberg S, Schapira M. BGP security in partial deployment: Is the juice worth the squeeze?//Proceedings of the 2013 ACM Conference on SIGCOMM. Hong Kong, China, 2013: 171-182

[119] Chan H, Dash D, Perrig A, Zhang H. Modeling adoptability of secure BGP protocols//Proceedings of the 2006 ACM Conference on SIGCOMM. Pisa, Italy, 2006: 279-290

[120] Siddiqui MS, Montero D, Serral-Graciä R, et al. A survey on the recent efforts of the Internet standardization body for securing inter-domain routing. Computer Networks, 2015, 80(0): 1-26

[121] Lepinski M. BGPsec protocol specification. draft-ietf-sidr-bgpsec-protocol-14, 2015

[122] Gagliano R, Retana R, Martinez C, Rada G. Implementing RPKI-based origin validation one country at a time — The Ecuadorian case study. draft-fmejia-opsec-origin-a-country-02, 2015

[123] Liu X, Yan Z, Geng G, et al. RPKI deployment: Risks and alternative solutions//Proceedings of the 9th International Conference on Genetic and Evolutionary Computing. Yangon, Myanmar, 2016: 299-310

[124] Cohen A, Gilad Y, Herzberg A, Schapira M. Jumpstarting BGP security with path-end validation//Proceedings of the 2016 ACM Conference on SIGCOMM. Florianopolis, Brazil, 2016: 342-355

[125] Yu H, Rexford J, Felten E W. A distributed reputation approach to cooperative Internet routing protection//Proceedings of the 1st IEEE ICNP Workshop on Secure Network Protocols (NPSec 2005). Boston, USA, 2005: 73-78

[126] Chang J, Venkatasubramanian K K, West A G, et al. AS-CRED: Reputation and alert service for inter-domain routing. IEEE Systems Journal, 2013, 7(3): 396-409

[127] Chang J, Venkatasubramanian K K, West A G, et al. AS-TRUST: A trust quantification scheme for autonomous systems in BGP//Proceedings of the 4th International Conference on Trust and Trustworthy Computing (TRUST 2011). Pittsburgh, USA, 2011: 262-276

[128] Konte M, Perdisci R, Feamster N. ASwatch: An AS reputation system to expose bulletproof hosting ASes. ACM SIGCOMM Computer Communication Review, 2015, 45(4): 625-638

[129] Hu Ning, Zou Peng, Zhu Pei-Dong. Reputation-based collaborative management method for inter-domain routing security. Journal of Software, 2010, 21(3): 505-515 (in Chinese)
(胡宁, 邹鹏, 朱培栋. 基于信誉机制的域间路由安全协同管理方法. 软件学报, 2010, 21(3): 505-515)

[130] Tan Jing, Luo Jun-Zhou, Li Wei, Yu Feng. Trust degree based inter-domain routing mechanism. Chinese Journal of Computers, 2010, 33(9): 1763-1774(in Chinese)
(谭晶, 罗军舟, 李伟, 于枫. 基于可信度的域间路由机制. 计算机学报, 2010, 33(9): 1763-1774)

[131] Wang Na, Wang Bin-Qiang. Internet autonomous system prefix reputation model. Computer Science, 2012, 39(9): 55-59(in Chinese)
(王娜, 汪斌强. 互联网自治系统的前缀信誉模型. 计算机科学, 2012, 39(9): 55-59)

[132] Xiong L, Liu L. PeerTrust: Supporting reputation-based trust for Peer-to-Peer electronic communities. IEEE Transactions on Knowledge and Data Engineering, 2004, 16(7): 843-857

[133] Jin-Hee C, Swami A, Ing-Ray C. A survey on trust management for mobile ad hoc networks. IEEE Communications Surveys & Tutorials, 2011, 13(4): 562-583

[134] Hendrikx F, Bubendorfer K, Chard R. Reputation systems: A survey and taxonomy. Journal of Parallel and Distributed Computing, 2015, 75(0): 184-197

[135] Gill P, Schapira M, Goldberg S. A survey of interdomain routing policies. ACM SIGCOMM Computer Communication Review, 2013, 44(1): 28-34

WANG Na, born in 1980, Ph. D., associate professor. Her research interests include network and information security.

DU Xue-Hui, born in 1968, Ph. D., professor. Her research interests focus on information security.

WANG Wen-Juan, born in 1981, Ph. D. candidate. Her research interests focus on network security.

LIU Ao-Di, born in 1992, M. S. candidate. His research interests focus on network security.

Background

The Border Gateway Protocol (BGP) is the de facto inter-domain routing protocol in the Internet, thus it plays a crucial role in current communications. Unfortunately, it is widely accepted that BGP does not provide any internal security mechanism, because the design of BGP was undertaken in the relatively homogeneous and mutually trusting environment of the early Internet. The intrinsic assumption of trust in the BGP protocol does not stand realistic anymore, as a number of day-to-day social as well as business applications, such as e-government affairs, online-banking, etc, increasingly rely on the Internet. Consequently, BGP is prone to a number of vulnerabilities and attacks, which can result in a traffic blackhole, or traffic interception/imposture, even lead to large scale outages in the Internet. In light of this, securing BGP has been an active research area.

The paper reviews research on BGP security in recent years. Firstly, the paper defines threat model, and analyzes in details prefix hijacking, path forging and routing leak; and then the paper reviews and summarizes the latest research progress on BGP security, which is divided into security extension and outsourcing techniques to defend prefix hijacking and path forging, techniques to defend routing leaking, and detection techniques to prefix hijacking, path forging and routing leaking, active response techniques, anomaly detection systems and BGP visualization tools; finally, discusses the challenges in the field of BGP security, and points out some future work to be done in terms of security defense, anomaly detection, interdomain routing trust and interdomain routing system measurement. This work is supported by the National Key Technologies Research and Development Program of China under Grant No. 2015AA011705 and Natural Science Foundation of Henan Province under Grant No. 162300410334.