软件学报 ISSN 1000-9825, CODEN RUXUEW
*Journal of Software*,2013,24(1):121−138 [doi: 10.3724/SP.J.1001.2013.04346]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

# BGP 安全研究*

黎 松[1], 诸葛建伟[2], 李 星[1]

[1](清华大学 电子工程系,北京 100084)

[2](清华大学 网络科学与网际空间研究院,北京 100084)

通讯作者: 诸葛建伟, E-mail: zhugejw@cernet.edu.cn

**摘 要**: BGP 是互联网的核心路由协议,互联网的域间选路通过 BGP 路由信息交换来完成.BGP 协议设计存在重大的安全漏洞,容易导致前缀劫持、路由泄漏以及针对互联网的拒绝服务攻击.分析 BGP 路由传播及路由策略等主要特性,揭示 BGP 协议的设计缺陷;探讨 BGP 面临的主要安全威胁,并对路由泄漏进行建模分析和界定特征;概括现有的 BGP 安全防御机制并指出其不足,进而对各种增强 BGP 安全的技术和方案进行合理分类和详尽研究,比较其利弊、剖析其优劣;最后,对 BGP 安全的未来研究趋势进行展望.

**关键词**: BGP;前缀劫持;路由泄漏;路由认证;前缀劫持检测

**中图法分类号**: TP393 **文献标识码**: A

中文引用格式: 黎松,诸葛建伟,李星.BGP 安全研究.软件学报,2013,24(1):121−138. http://www.jos.org.cn/1000-9825/4346.htm

英文引用格式: Li S, Zhuge JW, Li X. Study on BGP security. Ruanjian Xuebao/Journal of Software, 2013,24(1):121−138 (in Chinese). http://www.jos.org.cn/1000-9825/4346.htm

## Study on BGP Security

LI Song[1], ZHUGE Jian-Wei[2], LI Xing[1]

[1](Department of Electronic Engineering, Tsinghua University, Beijing 100084, China)

[2](Institute of Network Science and Cyberspace, Tsinghua University, Beijing 100084, China)

Corresponding author: ZHUGE Jian-Wei, E-mail: zhugejw@cernet.edu.cn

**Abstract**: BGP is a core Internet routing protocol. The Internet inter-domain routing relies on the exchange of BGP routing information. BGP has significant vulnerabilities, which have been found to cause problems such as prefix hijacking, route leak and Internet-targeted denial of service attack. First, by analyzing BGP route propagation and BGP routing policies, the fundamental flaw in the design of the protocol is revealed. The paper then discusses possible threats to BGP and presents a route leak model, which contributes to the description of its characteristics. Second, the existing defense mechanisms for BGP security are generalized, and their shortcomings are exposed. The paper then classifies various BGP security-enhancing technologies and studies them in detail to explore their advantages and disadvantages. Finally, the research trends of BGP security are discussed in this paper.

**Key words**: BGP; prefix hijacking; route leak; route validation; detecting prefix hijacking

BGP(border gateway protocol)协议是一种域间路由协议,也是 Internet 最为重要的路由协议之一.BGP 协议产生于 20 世纪 80 年代,当时,Internet 的前身——ARPANET 快速发展,为解决因网络规模急剧扩大而导致的路由可扩展性问题,RFC 827 提出一种解决方案,将 ARPANET 从一个单一协同管理的网络转化成由多个自治系统(autonomous system,简称 AS)分散互联的网络.自治系统又称为自治域,由独立实体管理.自治域内可自由选择 OSPF,RIP 等域内路由协议,自治域之间则采用相同的域间路由协议.最初的域间路由协议是在 ARPANET 中

* 基金项目: 国家自然科学基金(61003127); 国家重点基础研究发展计划(973)(2009CB320505)
收稿时间: 2012-03-01; 修改时间: 2012-09-12; 定稿时间: 2012-11-06; jos 在线出版时间: 2012-11-23
CNKI 网络优先出版: 2012-11-23 12:05, http://www.cnki.net/kcms/detail/11.2560.TP.20121123.1205.002.html

使用的 EGP(exterior gateway protocol)[1],EGP 协议可以说是 BGP 协议设计的雏形,它适用于早期基于骨干网的 ARPANET,仅支持树状拓扑结构的网络.随着互联网的拓扑结构逐渐由树状向网状互联转变,EGP 协议难以适应新的网络环境.此时,BGP 协议作为 EGP 协议的替代者便应运而生.

首个 BGP 协议版本在 RFC 1105 中制定.历经 IETF IDR 工作组的多次修改,目前,互联网中实际运行的版本为 BGP-4.BGP 协议是一种路径矢量(path vector)协议,它支持 CIDR、路由聚合以及灵活多变的路由选择策略.历史上,BGP 对于互联网的商业化和全球化立下了汗马功劳.然而,BGP 协议的设计在安全方面留有巨大的缺陷,这直接导致了互联网安全历史上多起重大事件的发生.比较知名的有 1997 年的 AS7007 误配事件[2]、2004 年的 TTNet 路由注入事件[3]、2008 年的 YouTube 劫持事件[4]以及 2012 年的澳洲网络中断事件[5].此外,BGP 协议的设计缺陷也使黑客对 BGP 协议的攻击兴趣日渐浓厚.例如,2008 年的 DEFCON 黑客大会,两位演讲者演示了对 BGP 协议进行中间人攻击以实现流量劫持的攻击方法[6].所有这些安全事件及攻击行为都充分暴露了 BGP 路由协议在安全上的脆弱性.

基于此,有关 BGP 安全的研究一直非常受人关注.在国家层面,美国国土安全部于 2003 年正式将 BGP 安全纳入网络空间国家安全战略[7],美国国家标准与技术研究院也在 2007 年制定了 BGP 协议安全标准文档[8].在学术界,BGP 安全也是网络安全领域的一个重要研究方向,许多研究者和安全组织一直在对其进行深入研究.比较典型的有 BBN 公司设计的 S-BGP[9]、Cisco 公司推出的 soBGP[10]以及 IETF 安全域间路由(secure inter-domain routing,简称 SIDR)工作组正在开发的 RPKI & BGPsec[11]协议.这些都为解决 BGP 安全问题提供了技术思路和努力方向.遗憾的是,由于 BGP 安全问题技术复杂而又牵涉面太广,BGP 安全至今仍是一个亟待解决的难题.

本文对 BGP 安全进行了系统而全面的深入研究,主要贡献如下:

(1) 统计分析历次重要的 BGP 安全事件,归纳讨论 BGP 面临的主要安全威胁;
(2) 剖析 BGP 的入站和出站路由策略,对因违反路由策略而导致的路由泄漏进行建模,并清晰地界定了路由泄漏的 3 个特征;
(3) 探讨现有的 BGP 安全机制,分析它们各自在保护 BGP 安全方面的作用并指出其不足;
(4) 对各种 BGP 安全增强研究进行了合理的分类,划分了 BGP 安全增强研究的主要方向,并对各个主要方向的研究进行技术与性能方面的综合比较;
(5) 指出了未来 BGP 安全研究的发展趋势和努力方向.

本文第 1 节概述 BGP 协议的主要特性.第 2 节介绍 BGP 协议的安全漏洞以及由此带来的各种安全威胁.第 3 节对现有的 BGP 安全机制进行概括和讨论.第 4 节对过往的 BGP 安全增强研究进行综合分类和详细比较.第 5 节展望 BGP 安全的未来研究趋势.第 6 节进行全文总结.

## 1 BGP 协议概述

BGP 是目前互联网实际使用的标准域间路由协议,它将为数众多、拓扑各异、大小不一的自治域连接在一起并相互交换路由信息.BGP 使用 TCP 作为路由交换的底层传输协议,其交换路由信息是以增量更新而非周期性更新的方式来进行.与其他路由协议相比,BGP 最主要的特性在于它具有独特的路由传播方式,同时,它还可以实现灵活多变的路由策略.

### 1.1 BGP的路由传播

作为路径矢量协议,BGP 在传播路由时携带有重要的路径信息.路径信息一方面用于指示到达该路由的网络拓扑,另一方面也用于路由选择.BGP 传播的路径信息主要包含网络层可达信息(network layer reachability information,简称 NLRI)和路径属性(path attribute).网络层可达信息包含 IP 前缀(prefix)和长度,用于标识目的网络的 CIDR 地址.路径属性描述到达该 CIDR 地址的路由的特殊属性.例如,AS_PATH 属性列出了到达目的网络所经过的一串 AS 路径,NEXT_HOP 属性说明了该路由的下一跳地址.

BGP 的路由传播过程如图 1 所示:两台 BGP 路由器通过 BGP 协议建立连接后成为 BGP 对等体,对等体之间通过 BGP Update 消息互相交换新的路由信息.获得的新路由经过路由过滤,并与现有路由表中的路由进行比

较,如果成为最佳路由,则该路由随后被传播到下一个 AS.如此相互传播下去,最终,所有相连的 AS 都将获知到各自所属网络的路由信息.

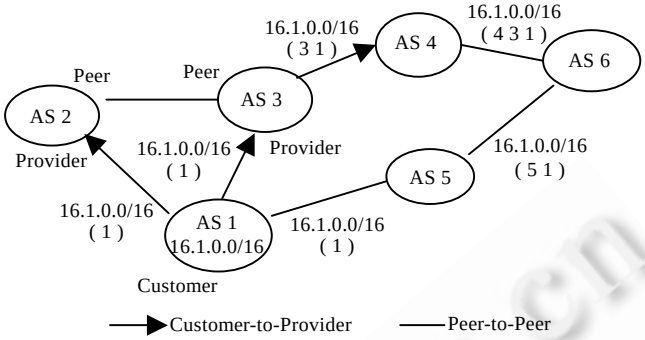



Fig.1 BGP route propagation

图 1 BGP 路由信息传播

### 1.2 BGP的路由策略

路由策略是指 AS 制定的接收路由、选择最佳路由以及对外通告路由的策略.BGP 对路由策略的丰富支持,是 BGP 协议得以成为互联网核心路由协议的关键.实际运营中,AS 通过设置 BGP 路由的路径属性来实现其路由策略.与路由策略相关的路径属性主要有 AS_PATH,LOCAL_PREF 和 MULTI_EXIT_DISC 属性.BGP 协议规定,LOCAL_PREF 值更高、AS_PATH 路径更短、MULTI_EXIT_DISC 值更小的路由会被选为最佳路由.

AS 路由策略的制定通常取决于 AS 之间的关系(AS relationships).互联网是一个分散自治的系统,AS 之间可以依据地理邻接和商业利益进行互联.互联的 AS 之间根据彼此的商业关系,执行相应的入站和出站路由策略来控制流量,其目的是实现各自商业利益的最大化.

AS之间的商业关系大致可分为4种:customer-to-provider(C2P),provider-to-customer(P2C),peer-to-peer(P2P)和 sibling-to-sibling(S2S)[12],其中,前 3 种关系最为重要.如上面图 1 所示,Provider AS 为 Customer AS 提供到其他 AS 的传输(transit)服务,Peer AS 之间则提供各自流量传输到对方网络的服务.假定一个 AS 的 provider,peer 以及 customer 都向其通告了到达同一网络的不同路由,则考虑到流量所产生的经济利益,AS 选择最佳路由的优先次序为 Customer>Peer>Provider.

此外,基于同样的经济利益考量,AS 通常还会制定如下的路由出站策略[13]:

1) 来自 customer 的路由通告给 customer,peer 以及 provider;
2) 来自 peer 的路由仅通告给 customer,不向 peer 和 provider 传播;
3) 来自 provider 的路由仅通告给 customer,不向 peer 和 provider 传播.

### 1.3 BGP的设计缺陷

客观来说,BGP 协议在路由功能上的设计非常稳健和可靠,这一点已被迄今为止 Internet 所表现出来的稳定性所证明.不过与之相比,BGP 协议在路由安全上的设计则显得有些薄弱.已有的研究[14,15]表明,BGP 协议在安全上存在着非常明显的设计缺陷和安全漏洞.

BGP 最主要的设计缺陷存在于 BGP 路由传播过程之中.按照 BGP 协议规范,BGP 在进行路由传播时,AS 只能向外通告自己所拥有的 CIDR 地址块.然而,由于 BGP 协议设计成默认接受对等体通告的任何路由,也即无条件信任对等体的路由宣告,这就导致即使一个 AS 向外通告不属于自己的前缀,也将会被对端接受并继续传播.这种错误的路由传播无疑会导致许多安全问题的发生.

BGP 的上述设计缺陷可以归结为 BGP 缺乏一个安全可信的路由认证机制,也即 BGP 无法对传播路由信息的真实性和完整性进行验证.

## 2 BGP 的安全威胁

BGP 运行于 AS 之间,理论上,互联网上的任意一个 AS 都可以通过 BGP 协议来影响其他任意 AS 的路由决策.这种紧密相关的特性犹如现实世界中的“蝴蝶效应”,容易使 BGP 协议乃至互联网因某一突发性的错误或攻击而遭受重大的安全威胁.

目前,研究者聚焦讨论最多的BGP安全威胁是前缀劫持(prefix hijacking),它起源于BGP在交换路由信息时缺乏可信路由认证机制这一主要设计缺陷;其次,由于 BGP 协议使用 TCP 传输路由信息,通过攻击 TCP 来威胁 BGP 通信也一直是人们研究的热点;再者,因近期互联网发生了多起造成网络大规模中断的路由泄漏(route leak)事件[5,16],路由泄漏也因此成为引人关注的一个新威胁.

图 2 是我们按时间顺序统计的重要 BGP 安全事件,每一事件都代表一种相应的安全威胁.以下我们对这 3 类威胁进行具体讨论.

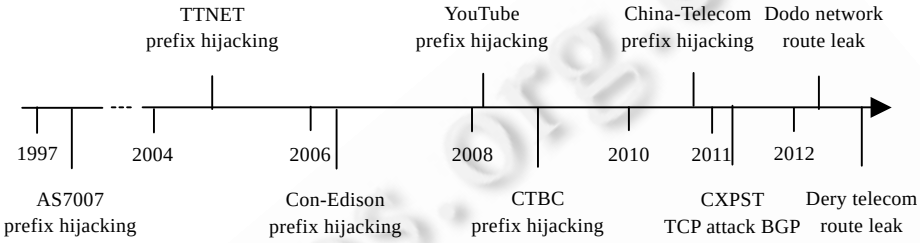



Fig.2 BGP security events

图 2 BGP 安全事件

### 2.1 前缀劫持

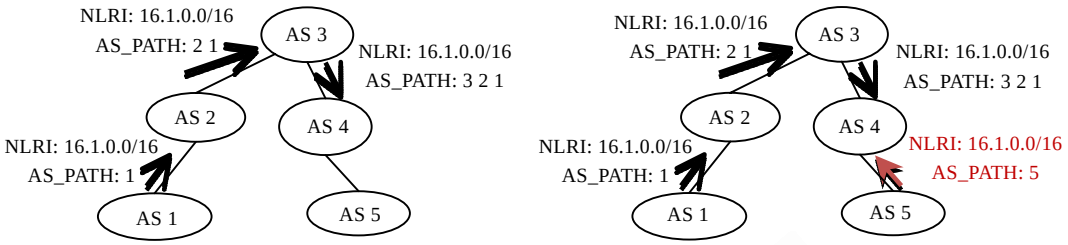
前缀劫持是指一个 AS 对外通告了一个未获授权的前缀.所谓“未获授权”是指该前缀属于其他 AS 所有或者该段地址空间尚未分配.Internet 地址分配遵循由 IANA 到 RIR(regional Internet registries)再到 LIR(local Internet registries)的授权层级,AS 违反授权对外通告非法的前缀将直接造成流量劫持的发生.例如,2006 年,AS27506(Con Edison 公司)[17]错误地通告了 AS2033(Panix 公司)拥有的 IP 前缀 166.84.0.0/16,造成流向 Panix 公司的部分流量被劫持到 AS27506.

过往的研究表明,前缀劫持的产生主要是由于管理员对 BGP 路由器进行了错误的配置[2,18],其原因大多与 IGP(interior gateway protocol)到 BGP 的路由重分发(redistribute)有关.然而,2008 年,巴基斯坦电信为限制其国内用户访问 YouTube 网站,对 YouTube 的前缀进行了恶意的主动劫持.自那以来,研究界对这种恶意前缀劫持行为的研究越来越多.一般而言,恶意攻击者可以通过伪造 NLRI 信息和 AS_PATH 路径来达到成功实施前缀劫持的目的.

#### 2.1.1 伪造 NLRI 信息

此种情况下,恶意的 AS 伪造 BGP Update 消息中的 NLRI 信息,向外通告一个非法的前缀.如图 3(a)所示,AS1 是前缀 16.1.0.0/16 的合法拥有者,它向外通告到达该段网址的路由.在图 3(b)中,AS5 恶意伪造 NLRI 也向外通告到达 16.1.0.0/16 的路由.如此,根据 BGP 选取最短 AS_PATH 路径的原则,AS4 将优先选取经 AS5 到 16.1.0.0/16 的路径.

更进一步地,如果攻击者不但伪造 NLRI 中的前缀,而且修改成一个更长的前缀长度,那么依据 BGP 的最长匹配原则,所有其他的 AS 将选择该伪造路径,如图 4 所示.




(a) AS1 通告合法的 16.1.0.0/16　　(b) AS5 通告伪造的 16.1.0.0/16

Fig.3　Falsify NLRI prefix

图 3　伪造 NLRI 信息中的前缀

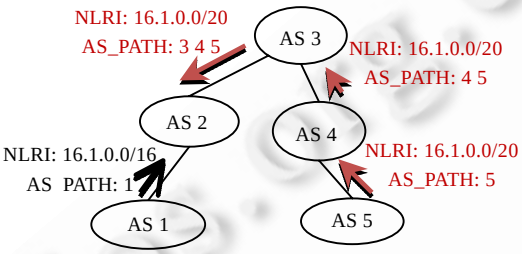



Fig.4　Falsify NLRI prefix and length

图 4　伪造 NLRI 信息中的前缀及长度

2.1.2　伪造 NLRI 信息和 AS_PATH 路径

上述伪造 NLRI 信息实施前缀劫持的攻击方式会造成多源 AS(multiple origin AS,简称 MOAS)冲突[19],即一个前缀被多个 AS 通告.MOAS 冲突容易被已有的各类 BGP 监测工具[20,21]检测出来.为避免此类监测,攻击者可通过同时修改 NLRI 信息和 AS_PATH 路径来解决 MOAS 问题.如图 5 所示,AS 5 伪造前缀 16.1.0.0/16,同时准备修改 AS_PATH.为避免产生 MOAS,攻击者可将 AS_PATH 直接修改为{1},但这样通告的路由会被 AS 4 拒绝,原因是 BGP 规定 AS_PATH 属性的最后一跳 AS 要与通告路由器本身的 AS 号(此处为 5)一致.可行的修改方式是将 AS_PATH 修改为{5 … 1}之类的起源为 1,最后一跳为 5 的路径,这里假设 AS_PATH 被修改成{5 1}.如此,AS 4 将收到两条到达 16.1.0.0/16 的 AS_PATH 路径{3 2 1}和{5 1},依据最短路径原则优先选择经 AS 5 到达 16.1.0.0/16.这样,AS 4 中目的地为 16.1.0.0/16 的流量原本应该路由到 AS 1 中,却被劫持到了 AS 5 中.

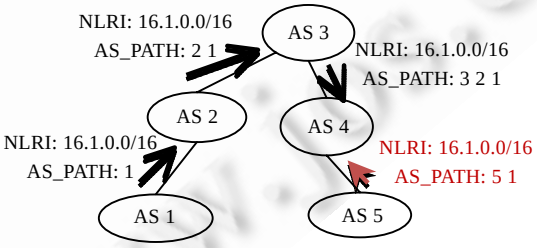



Fig.5　Falsify NLRI and AS_PATH

图 5　伪造 NLRI 信息和 AS_PATH 路径

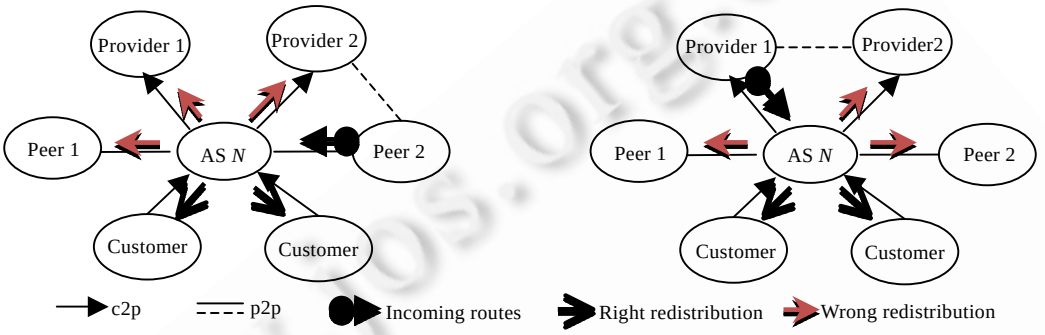
总而言之,前缀劫持是 BGP 协议面临的最主要的威胁,其结果轻可造成路由黑洞(black hole)和中间人攻击(man-in-the-middle attack,简称 MITM),重则容易导致互联网的大规模瘫痪.

### 2.2 路由泄漏

路由泄漏是一种能够造成 BGP 路由发生严重错误、进而导致互联网部分中断的重要威胁.鉴于最近几起路由泄漏事件的破坏性,路由泄漏在近期逐渐为研究人员所关注.目前,研究界对路由泄漏尚未有确切的定义,文献[22]尝试对其给出定义,但未获 IETF SIDR 工作组的认可.本文在此对路由泄漏进行一个初步的界定.

我们界定路由泄漏的依据主要来源于对具体路由泄漏事件[5,16]的综合调查.利用 RouteViews[23]和 RIPE RIS[24]收集的 BGP 路由历史数据,我们对这些泄漏事件进行了充分的取证分析,并建立了如图 6 所示的两种路由泄漏模型.

图 6(a)和图 6(b)分别表示违反 peer-to-peer 路由策略和违反 provider-to-customer 路由策略的两种路由泄漏.在图 6(a)中,AS *N* 将接收自 peer 的路由通告给了它的 provider 和另外的 peer;图 6(b)中,AS *N* 将接收自 provider 的路由通告给了它的 peer 以及另外的 provider.这两种路由通告行为虽然都符合 BGP 协议的路由传播规范,但却明显违反了我们在第 1 节中介绍的 BGP 路由出站策略.




(a) 违反 peer-to-peer 路由策略 (b) 违反 provider-to-customer 路由策略

Fig.6 BGP route leak

图 6 BGP 路由泄漏

依据文献[12]构建 AS 图 $G=(V,E)$的方法,我们以 *r* 代表 AS *N* 路由表中的每条 BGP 更新路由,*r.last_as* 代表该路由 AS_PATH 中最左边的 AS,也即通告该路由的上一个 AS.以 *export*(*M*,*N*)代表 AS *N* 到 AS *M* 的出站路由策略,*export*(*M*,*N*)[*r*]代表 AS *N* 对路由 *r* 应用出站路由策略后向 AS *M* 通告的路由.同时,以 *provider*(*N*),*peer*(*N*),*customer*(*N*)分别代表 AS *N* 的 provider,peer 以及 customer,则上述路由泄漏模型可以表示为

$$export(M,N)[\{r \mid r.last\_as \in provider(N) \cup peer(N)\}] \neq \varnothing \quad \text{if } M \in provider(N) \cup peer(N).$$

路由泄漏通常会造成流量重定向.例如在图 6(a)中,假设 peer 2 与 provider 2 互联且为 peer-to-peer 的关系,peer 2 的 prefix 被 AS *N* 违反策略“泄漏”给了 provider 2.此时,provider 2 的路由表中有两条到达 peer 2 prefix 的路由,一条来自 peer(peer 2),另一条来自 customer(AS *N*).根据第 1 节所描述的选择最佳路由的优先次序 Customer>Peer>Provider,则 provider 2 将舍弃直连到达 peer 2 的路径,转而选择经 AS *N* 到达 peer 2 网络,这就造成 provider 2 访问 peer 2 网络流量的重定向.同理,在图 6(b)中,路由泄漏也会使得从 provider 2 访问 provider 1 的流量重定向到 AS *N*.

综合上述分析,我们可以归纳出路由泄漏的 3 个特征:

(1) 路由泄漏通告的路由合法,因此路由泄漏不属于前缀劫持的范畴;

(2) 路由泄漏通告的路由明显违反了 AS 之间的路由策略;

(3) 路由泄漏的后果是造成流量重定向.

### 2.3 TCP协议带来的安全风险

BGP 使用 TCP 协议作为传输层,自然,针对 TCP 协议的攻击手段都将给 BGP 安全带来风险.传统的 TCP

SYN,TCP SYN ACK,TCP ACK,TCP RST/FIN/FIN-ACK 等各种 TCP 攻击方式,都可能用于威胁 BGP 会话的安全[14].此外,从信息安全的角度来说,对 TCP 会话保密性和完整性的攻击也会给 BGP 安全造成重大影响[25].通过这两种攻击,攻击者可以窃听 BGP 路由信息,推断 AS 之间的商业关系;还可恶意删除、修改以及重播 BGP 消息,造成 BGP 路由的撤销和震荡,进而引起网络中断.

近来,针对 BGP 协议的 TCP 攻击有了新的发展.借助于 Kuzmanovic 等人[26]提出的 Low-rate TCP-targeted DoS 攻击方式,Zhang 等人[27]避开 BGP 的安全防御机制,对选定的 BGP 链路实施数据平面的远程拒绝服务攻击.由于 BGP 会话的控制平面与数据平面共享同一信道,数据平面的 TCP 会话拥塞必然引起控制平面的 TCP 拥塞,因此,受攻击的 BGP 会话将被重置,进而引起路由撤销和网络不可达.这种新的 BGP 攻击方式以 3 位作者的名字被命名为 ZMW 攻击,并且一出现就引起研究人员的关注.

Schuchard 等人[28]进一步拓展了 ZMW 攻击的方式和效果,他们通过僵尸网络(botnet)对多个 BGP 会话同时发起协作式跨平面会话终止(coordinated cross plane session termination,简称 CXPST)攻击.这种攻击将使 BGP 会话因反复重置而产生大量的 BGP 更新消息.这些巨量的 BGP 更新将被传播到互联网的所有核心路由器,引起路由器的 CPU 过载,进而严重影响互联网的路由性能.Schuchard 等人展示的这种攻击被媒体形象地称为“数字大炮(digital ordnance)”.

## 3 BGP 的安全机制

上节所描述的众多安全威胁,促使 BGP 协议不断地更新和完善.经研究者和 BGP 开发人员的共同努力,BGP 发展了很多加强协议安全性的机制.然而,并非所有的安全机制都能适应互联网这个分散自治的系统,考虑到性能开销以及现实部署等多方面的原因,目前已经得以应用的安全机制并不多.概括而言,AS 常用的 BGP 安全机制主要包括 TCP MD5[29]、GTSM(generalized TTL security mechanism)[30]、路由抖动抑制(route flap damping)、路由过滤(routing filtering)以及路由注册(routing registries)这 5 种.

### 3.1 TCP MD5

TCP MD5 是 Cisco 公司在 RFC 2385 中提出的一种用于保护 BGP 会话的签名选项.该方案在每个 TCP 段中加入了一个包含 MD5 摘要信息的扩展项.用于计算 MD5 摘要的内容包括 TCP 伪首部、首部、数据段以及一个对话双方独立共享的密钥.接收者使用本地密钥按照相同的算法计算 MD5 摘要,并与接收到的摘要相比较,相同则接受,不同则丢弃此数据.

TCP MD5 签名选项在一定程度上可以保证 BGP 会话消息的真实性、完整性以及抗重播性,但显然无法保证会话的机密性.此外,MD5 算法在今天看来也并不安全,它本身存在产生“碰撞”[31]的问题.而且,对 MD5 算法的破解也发展成采用彩虹表(rainbow)查表的方式[32],这使 MD5 算法的安全性大为降低,进而相应地减弱了使用 TCP MD5 签名选项的安全效果.

### 3.2 GTSM

GTSM 是一种对数据包的 *TTL* 值进行检测,进而判别攻击威胁的安全机制.它利用 IP 数据包经过路由器时 *TTL* 值减 1 这一原理,通过鉴别接收数据包的 *TTL* 值来抵御外部攻击.GTSM 机制比较适用于会话双方直接相连的协议.由于 BGP 会话大都是点到点连接,所以 GTSM 可以很好地应用于 BGP.具体来说,采用 GTSM 机制的 BGP 路由器发送数据包时将 *TTL* 值设为最大值 255,接收数据包的 BGP 对等体检查数据包的 *TTL* 值,若该值等于 255,则接受,否则,丢弃.

根据上述原则,GTSM 可以有效防止针对 BGP 路由器的远程攻击.远程攻击者通常处于与被攻击路由器距离 1 跳以外的位置,无论它采取包括 IP 欺骗在内的何种攻击手段,攻击数据包到达被攻击路由器时的 *TTL* 值都将小于 255,攻击数据包将因此而被 GTSM 机制拒绝接收.

GTSM 机制简单、有效,它对 BGP 会话的安全起到重要的保护作用.不过,在实际配置时,考虑到 IBGP 可以不直连以及 EBGP 可能使用多跳连接等因素,GTSM 的 *TTL* 判别阈值需要做出相应的调整.

### 3.3 路由抖动抑制

路由抖动是指BGP路由反复被通告而后又被撤销的现象.频繁的路由抖动将增加路由器的CPU负担,同时影响BGP路由的可达性,进而可能造成网络不稳定而发生中断.为此,RFC 2349提出了路由抖动抑制的方法来解决该问题[33].该方法对抖动的路由分配一个惩罚值,惩罚值随抖动次数的增多而增大,当惩罚值增大到抑制门限(suppress limit)时,该路由将被抑制,停止向外通告.

路由抖动抑制一直以来都被当作增强BGP路由系统稳定性的机制,不过后来的研究[34]表明,路由抖动抑制会显著地影响路由收敛时间,而且因为不同路由器厂商对MRAI(minimum route advertisement interval)时间设置的差异,路由抖动抑制反而有可能造成正常的路由通告被错误抑制[35].

### 3.4 路由过滤

路由过滤是现阶段用于保护BGP安全的最重要的手段.AS应尽可能地根据自己的路由策略制定详细的入站和出站路由过滤规则.事实上,历次BGP安全事件的调查分析均表明,没有实施正确的路由过滤是导致事件发生的重要原因.鉴于此,很多研究详细讨论了用于路由过滤的基本原则[25,36,37].一般而言,以下这些指导规范ISP应该遵循:

(1) 过滤bogon地址:bogon地址是指IANA及RIR尚未授权分配的地址.由于地址分配每天都在进行,所以过滤此类地址需要及时到相关的数据库[38]进行更新;

(2) 过滤特殊地址:特殊地址主要包括私有地址、回环地址、组播地址以及IPv6的链路本地地址等;

(3) 过滤前缀长度过长的地址:IPv4前缀长度超过/24,IPv6前缀长度超过/48的通常应被过滤;

(4) 过滤ISP自身地址:对ISP自身地址实施入站过滤可以防止内部流量被劫持;对ISP内重要的网络基础设施,比如关键服务器、网络管理主机等设备的地址实施出站过滤,防止它们被外部非法访问;

(5) 过滤customer地址:对来自customer的路由实施严格的入站过滤,只接收customer本身所拥有的prefixes,含有其他prefix的路由一律拒绝.这一条过滤规则非常重要,严格实施此规则可有效防止前缀劫持和路由泄漏事件的发生.

### 3.5 路由注册

路由注册(routing registries)是指AS将自己的路由信息、路由策略注册到公共数据库以便相互查询的行为.目前,使用较为广泛的路由注册数据库主要是1995年建立的IRR(Internet routing registry)[39],该数据库储存了以RPSL(routing policy specification language)[40]语言描述的相关信息.这些信息由AS各自维护建立,记录了AS的地址列表、入站和出站策略等内容.

通过查询IRR数据库,AS不但可以鉴别路由的起源,还可以验证该路由是否违反了AS之间的路由策略,这一点对AS防止前缀劫持和路由泄漏都很有益.不过,IRR在运营中存在一些问题,影响了它的实际使用效果.这些问题主要包括:

(1) IRR数据库的内容不完整:路由注册采取自愿原则,并非所有的AS都愿意向IRR数据库注册自己的路由信息;而且,路由策略涉及商业机密,参与注册的AS会有所保留地注册自己的数据;

(2) IRR数据库的内容不可靠:随着时间的推移,AS的地址列表、路由策略都会发生变化.这些变化不能及时更新到IRR数据库中,导致IRR数据库的内容与现时情况存在差异;

(3) IRR数据库不安全:IRR数据库系统缺乏认证与授权措施,容易导致数据遭到篡改.IETF已经制定了相应的RPSS(routing policy system security)[41]机制,但该机制目前尚未在IRR系统中得到支持.

上述这些问题引起了一些研究人员的关注,Liu等人提出一种E-IRR[42]机制,从提高实用性和安全性的角度出发设计一种前缀策略(prefix policy)注册数据库,用于更好地防范前缀劫持.

## 4 BGP的安全增强研究

上节所讨论的BGP安全机制可在一定程度上保护BGP的安全,但要彻底解决BGP安全问题还需要进一

步深入地加以研究.这一方面是因为 BGP 协议在安全上的设计缺陷仍然存在,研究者仍然需要为弥补这一设计缺陷而努力提出各种技术方案;另一方面也是基于BGP对互联网牵一发而动全身的重要地位,任何一种BGP安全技术都需要认真考虑性能开销、增量部署(incremental deployment)等可行性问题.

概括而言,当前绝大多数的 BGP 安全增强研究都致力于解决前缀劫持这一根本性的问题.这些研究大致可以分为两个方向:一是给BGP协议的安全漏洞"打补丁",即通过采用各种路由认证技术来修补BGP协议缺乏路由认证机制的缺陷;二是借鉴入侵检测的思想发展各类 BGP 前缀劫持检测技术,在前缀劫持事件发生后及时发现并解决问题.下面我们分别从这两个方面对现有的各类 BGP 安全技术加以详述.

### 4.1 路由认证技术

IETF 的 SIDR 工作组将 BGP 的路由认证分解为两个问题:

A. 一个 AS 是否拥有通告某一 IP 前缀的合法授权(origin AS 的真实性)?

B. 一条 BGP 路由中的 AS_PATH 是否与其 NLRI 实际传播的路径一致(AS_APTH 的完整性)?

这两个问题实际上分别代表路由信息的真实性和完整性两个方面,解决了这两个问题就等于基本上消除了前缀劫持的安全威胁.围绕这两个问题的解决,涌现出了相当多的技术思路.首先,最容易想到的思路是引入PKI 对 BGP 路由消息进行数字签名.数字签名经过多年的发展已被证明是解决身份认证问题最有效的方法.不过,由于数字签名的计算开销较大以及建立和部署 PKI 的难度,又有人研究以对称密钥加密来替代 PKI 的技术.当然,除此之外还有一些其他的另辟蹊径的办法,比如较早的基于 DNS 的 NLRI 信息源认证技术[43]以及基于本地路由注册思想的 IRV[44]技术,等等诸如此类.受篇幅所限,本文将选择最有影响力和代表性的一些技术方案进行分析.

#### 4.1.1 S-BGP

Kent 等人提出的 S-BGP(secure BGP)[45]是使用 PKI 技术来增强 BGP 安全性的最早的文献之一.通过建立一套用于证书发布和路由验证的 PKI,以及引入一种新的可选传递(optional transitive)路径属性,S_BGP 构建了一个完整的解决 BGP 路由认证问题的架构.具体来说:

首先,IP 地址分配和 AS 号码分配都是依照从 IANA 到 RIR 再到 ISP 这一模式沿袭下去,S-BGP 借鉴了该模式并建立了一套与之并行的 PKI 体系.IANA 作为此体系的信任起点,为 RIR 签发证书,RIR 继而为 ISP 签发证书.一个 ISP 有两种证书:IP 地址块证书和 AS 号码证书.IP 地址块证书将 ISP 的公钥与其申请的 IP 地址空间绑定,表明这些 IP 地址空间归该 ISP 拥有;AS 号码证书则将 ISP 的公钥与其申请的 AS 号码绑定,表明这些 AS 号码属该 ISP 所有.

其次,ISP 也作为 CA 分别为其所管理的各个 AS 和 BGP 路由器签发证书,这两类证书用以鉴别 AS 和 BGP 路由器的身份.

为了能使用上述证书对 BGP 路由进行认证,S-BGP 还设计了两类证明(attestations):地址证明(address attestations)和路由证明(route attestations).这里所谓的"证明(attestation)"是一段数字签名数据,其格式在文献[46]中给出定义,如图 7 所示.

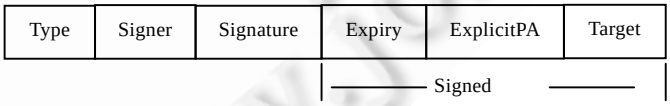



Fig.7 Structure of an attestation

图 7 Attestation 数据格式

"地址证明"的 Signer 是 ISP,ExplicitPA 字段包含有该 ISP 拥有的一段 IP 前缀,Target 是 ISP 授权用于通告该 IP 前缀的 AS 号.ISP 使用其私钥对 IP 前缀和 AS 号码数据进行签名并置于 Signature 字段,以保护该段数据的完整性和真实性."地址证明"实际上表明了哪个 AS 被 ISP 授权来通告其所拥有的前缀.

“路由证明”的格式和“地址证明”的格式一样.“路由证明”的 Signer 是 BGP 路由器,ExplicitPA 字段含有要通告的 IP 前缀,Target 是路由器对等体的 AS 号.“路由证明”用 BGP 路由器的私钥进行签名,“路由证明”实际上代表了 BGP 路由通告方对其对等体继续通告该 IP 前缀的授权.值得注意的是,S-BGP 将“路由证明”设计为一种新的路径属性,随 update 消息传送.

利用上述 4 种证书和两种证明,BGP 路由器可以实现对接收到的 BGP 路由进行认证.方法是:提取路由信息中的 IP 前缀,从其他地方获取与该 IP 前缀绑定的 ISP 证书和“地址证明”,用 ISP 的公钥验证“地址证明”,就可证实路由的 origin AS 是否具有通告该前缀的合法授权;对于 AS_PATH 的认证,则可使用 AS_PATH 中每一跳 AS 的路由器证书来对路由消息中携带的“路由证明”逐个验证,以证实该 AS_PATH 确实可信.

S-BGP 虽然成功地解决了路由认证问题,不过也相应地带来计算开销大、路径收敛时间延长的问题[47],更加上建立 PKI 需要 IANA、RIR、ISP 以及路由器厂商的共同参与,致使 S-BGP 始终未能实际部署.

#### 4.1.2 soBGP

针对 S-BGP 存在的问题,Cisco 公司提出了一套更为简洁的 BGP 安全方案——soBGP(secure origin BGP)[48].soBGP 设计了 3 类证书来实现路由认证:EntityCert,AuthCert(authorization certificate)和 ASPolicyCert.其中,EntityCert 证书用于鉴定 AS 实体身份,颁发给每个 AS,并将其 AS 号绑定到一个公钥,由第三方进行签名.该证书的身份验证基于网状信任模型(Web of trust),可以依赖于 VeriSign 这样的知名认证服务提供商的公钥来认证.

AuthCert 证书用于给 AS 提供通告一个 IP 地址块的授权.AuthCert 将该 AS 和它可能通告的地址块相关联.AuthCert 证书采用 TLV(type/length/value)格式和逐级授权机制.如图 8 所示,地址块所有者的上一级 AS 给下一级 AS 授权签名,证书的验证可以通过追溯上一级 AS 的公钥进行,如此逐级往上,完成地址块和通告 AS 的分配.

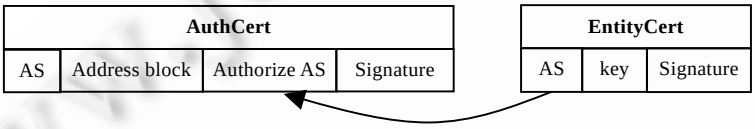



Fig.8 Authorization for advertising a block of address

图 8 授权 AS 通告地址块

ASPolicyCert 证书用于描述 AS 之间的拓扑连接关系.每个 AS 将其连接的各个对等体列表于该证书中,并使用其私钥签名,所有 AS 根据这些 ASPolicyCert 证书建立 AS 连接拓扑图.依据此拓扑图,AS 可以判断路由中的 AS_PATH 路径是否属实.ASPolicyCert 证书可以说是 soBGP 方案最为巧妙的一个设计.

所有上述 3 类证书都使用 soBGP 设计的一种名为 SECURITY Message 的新的 BGP 消息类型来传送.

soBGP 的设计力图减轻由于增强安全性而带来的负面开销,它没有采用 S-BGP 的层次结构信任模型,因而也就不需要建立专门的 PKI 体系.然而也正因为如此,缺乏信任锚的地址授权认证体系使 soBGP 的安全性显著地降低[49].

#### 4.1.3 IRV

IRV(interdomain routing validation)[44]是一种结合 S-BGP 和 IRR 思想的 BGP 安全方案.在 IRV 架构中,一个 AS 可以向其他 AS 证明自己曾经通告和传播过的路由,其他 AS 获取这些信息来对接收到的路由进行验证.具体来说,每个 AS 都专门提供一台验证服务器,该服务器充当“域间路由验证器(interdomain routing validator)”的角色.验证服务器中记录有本地 AS 路由策略信息、本地 AS 接收到的路由通告以及本地 AS 发送过的路由通告等信息.当其他 AS 需要对某一接收路由进行验证时,可以向该 AS 的验证服务器查询历史路由通告记录,以核对路由的有效性.

如图 9 所示,假设 AS 4 收到一条前缀为 16.1.0.0/16,AS_PATH 为{3 2 1}的路由通告.为验证 AS 1 是否是该路由的发起者,AS 4 可以向 AS 1 的 IRV 验证服务器查询路由记录,以证明 AS 1 确实通告了此前缀.同时,为验证

AS_PATH 路径,AS 4 可以逐个地向 AS 1,AS 2,AS 3 发起查询,求证 AS 1 是否将路由传播给了 AS 2,而 AS 2 又将路由传播给了 AS 3.

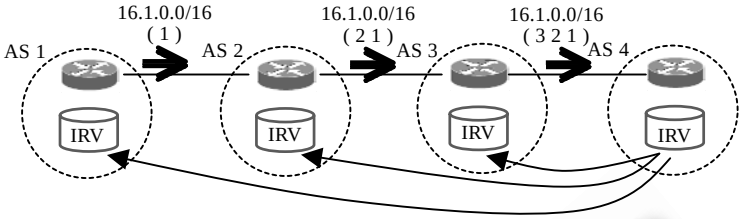



Fig.9 Process of IRV route validation

图 9 IRV 路由验证过程

IRV 的上述设计看似简单有效,然而却存在几个重要的缺陷不容回避:其一,如何确保 IRV 验证服务器信息的真实性和完整性?如果本地管理员错误地配置了路由信息或服务器遭到恶意攻击导致信息错误,那将使路由验证结果变得不可信;其二,IRV 可以向其他 AS 证明自己是某个路由通告的发起者,但它无法证明这一路由通告中的 IP 前缀确实归它所有,IRV 方案本身也承认,要解决这一问题依然需要类似 S-BGP 那样的地址证书.

#### 4.1.4 RPKI & BGPsec

RPKI & BGPsec 是目前 IETF SIDR 工作组正在开发的域间路由安全标准.RPKI(resource public key infrastructure)[50]是一种“资源公钥基础设施”,用于证书的发布以及对路由通告合法性的验证.BGPsec[51]是一项 BGP 安全扩展,其目的是为 BGP update 消息中的 AS_PATH 属性提供安全保护.RPKI 与 BGPsec 结合,用以对 BGP 路由的真实性和完整性进行验证.

从 SIDR 工作组目前发布的部分 RFC 文档及草案来看,RPKI & BGPsec 基本沿袭了 S-BGP 方案的技术思路,即主要依靠数字签名和证书来增强 BGP 协议安全.RPKI 的证书发布体系与现有的地址分配和 AS 号码分配体系相吻合,它从 IANA 和 RIR 向下逐级签发资源证书,直到端实体(end entity).端实体拥有一段不可再细分的 IP 地址资源,它使用自己的私钥为一段名为路由源授权(route origination authorizations,简称 ROA)的信息进行签名.ROA 包含端实体的 IP 地址块以及端实体指定用于通告该段地址的 AS 号.

所有证书以及 ROA 均通过一套分布式的 RPKI 证书库系统(RPKI repository system)进行集中和分发,每台 BGP 路由器都可以从自己所属的 ISP 分发点获取各类证书和 ROA.利用端实体证书对 ROA 信息进行认证,就可以验证 AS_PATH 中的 origin AS 是否有通告 NLRI 的授权.这一过程如图 10 所示.

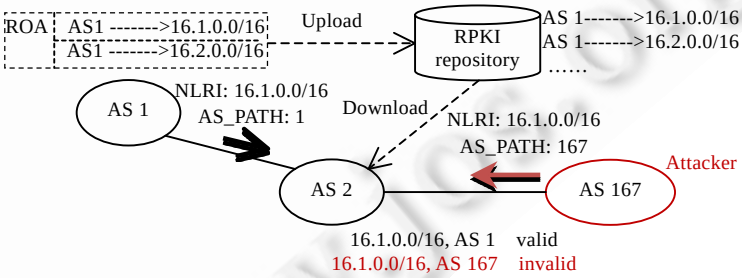



Fig.10 Validate origin AS using RPKI

图 10 使用 RPKI 验证 origin AS 的授权

RPKI 中的 ROA 实际上相当于 S-BGP 中的“地址证明”.同理,BGPsec 新引入的路径属性 BGPSEC_Path_Signatures 也相当于 S-BGP 中的“路由证明”.BGPSEC_Path_Signatures 实际上代表了 AS_PATH 中的前一 AS 对后一 AS 继续通告路由的授权,签名和验证方式也与 S-BGP 中大致类似,这里不再赘述.

4.1.5 ROVER

ROVER(route origin verification)[52]是最近提出的一种新的验证 BGP 路由真实性的技术.它的基本思想是,利用反向 DNS 查询来验证 AS 是否具有通告相应 prefix 的授权.反向 DNS 查询通常只能查询一个 IP 地址,而不能查询一段 IP 地址块.ROVER 的创新在于,它设计了一种编码机制[53],可将一段任意长度的 IP 地址块添加到一项新设计的 SRO[54]反向查询资源记录当中.这种 SRO 资源记录的示例如下:

1.16.in-addr.arpa. 86400 IN SRO 4538

它的含义是授权 AS4538 作为 16.1.0.0/16 的合法通告者.这样,当其他 AS 收到 prefix 为 16.1.0.0/16 的路由通告时,就可以通过查询 1.16.in-addr.arpa 的反向 DNS 资源记录得到 16.1.0.0/16 的合法通告 AS 号,并由此验证这条 BGP 路由通告的真实性.

从实际应用的角度来看,ROVER 技术很容易部署,它不需要对现有的 BGP 协议作任何修改,只需对 DNS 反向查询区进行简单的扩展即可.当然,为了保证这种 DNS 反向查询结果的可信,ROVER 需要依赖于 DNSSEC[55]的支持.

4.1.6 其他路由认证研究

有关 BGP 路由认证的其他研究多数以 S-BGP 为参考来进行.鉴于 S-BGP 无法在增强安全与降低开销及部署难度方面取得平衡,这些研究主要围绕以下几个方面来探索:

(1) 安全且高效的 origin AS 认证[56];

(2) 安全且高效的 AS_PATH 认证[57,58];

(3) 简单、易部署的 PKI 体系[59,60];

(4) 轻量级的认证技术[61].

总之,这类研究均着眼于如何改进 S-BGP 的两大缺陷,即:需要建立和部署复杂 PKI 体系的问题以及相应的由于采用非对称加、解密技术所带来的计算开销问题.

### 4.2 前缀劫持检测技术

前缀劫持检测是 BGP 安全领域的另一个研究热点,同样存在众多不同的技术方案.实际上,大多数的方案都是基于前缀劫持的以下两个重要特征来研究相关检测技术:

A. MOAS 冲突:即一个 prefix 匹配多个 origin AS 的行为.这是前缀劫持之于路由控制平面最重要的一个特征;

B. IP 地址冲突:在数据平面层次上,前缀劫持直接导致了一个目的 IP 地址(被劫持的前缀)存在多个不同的路由目的地的问题.也就是说:假设 16.1.0.0/16 为 AS 1 所有,但被 AS 2 劫持,则目的地址为 16.1.0.0/16 的数据包可能分别从 AS 1 和 AS 2 返回.或者,源地址为 16.1.0.0/16 的数据包可能有去无回(返回数据包被路由到 AS 2).

基于上述两个特征,一类检测技术重在研究如何实时发现 MOAS 冲突,并进而判别是否发生了前缀劫持;另一类检测技术使用主动探测手段,通过发送各种探测数据包并基于其响应来判断是否发生了前缀劫持.下面分别从 MOAS 检测和主动探测两个方面归类叙述.

4.2.1 MOAS 检测技术

MOAS 检测技术从控制平面提供的信息来检测前缀劫持的威胁.MOAS 检测研究最早见于文献[19],该文献将 MOAS 冲突划分为有效的 MOAS 和无效的 MOAS.有效的 MOAS 可能由于多宿主(multi-homing)等因素所造成,无效的 MOAS 则由前缀劫持所产生.MOAS 检测技术的核心在于如何快速、准确地检测出无效的 MOAS 冲突.比较有影响的 MOAS 检测技术包括如下几种:

(1) MOAS List

MOAS List[62]是一种相对简单的 MOAS 检测机制.MOAS List 的基本思想是:创建一个包含所有授权通告某一前缀的 origin AS 的列表(MOAS list),将该列表附于每一授权 AS 的路由通告中.当其他路由器接收到关于这一前缀的所有路由通告时,比较通告中的 MOAS List 是否一致,以此判断是否发生了前缀劫持.

MOAS List 技术之所以有效,主要在于 Internet 是一个高度互联的 mesh 网络.无论是因恶意攻击还是因管理员误配所产生的前缀劫持,由于 BGP 路由传播的多路径特性,错误的 MOAS List 和正确的 MOAS List 最终都会被接收路由器收到,两者的不一致就会使接收路由器意识到发生了前缀劫持事件.

(2) PHAS(prefix hijack alert system)

PHAS[63]是目前得以实际应用的另一类 MOAS 检测技术的典型代表.它通过审查诸如 RouteViews 之类的 BGP 监测项目收集的路由数据,发现前缀劫持威胁并实时地向前缀所有者通报.PHAS 的设计理念认为,当出现 MOAS 冲突时,只有前缀所有者才能准确地分辨出是合法的 MOAS 还是前缀劫持.基于此,PHAS 建立了一个完整的劫持检测及通知架构:用户首先向 PHAS 系统注册自己想要保护的前缀,系统将依据 RouteViews 的数据对该前缀进行监测.当发现前缀的起源发生变化时,系统将通过邮件等渠道向用户发出警告,用户根据警告提供的信息来判断是否发生了前缀劫持.

PHAS 的优点是设计简单、部署容易且很有效;缺点是在缺乏 PKI 的情况下无法验证用户对其注册的前缀的所有权,存在恶意攻击者冒称某一前缀所有权的可能.

(3) PGBGP(pretty good BGP)

PGBGP[64]由 Karlin 等人提出.该方案建议 BGP 路由器审慎地应对 MOAS 冲突.方案从改变路由器的决策规则着手,延迟可疑路由被采用和向外传播的时间,以最大限度地减少前缀劫持可能带来的损害.方案的核心在于如何定义可疑路由和正常路由.他们为此采用的方法是:首先,在一段历史时间(history period)内收集所有接收的 update 消息,通过结合 update 消息内容和路由器的 RIB,提取 update 消息中每一前缀对应的 origin AS;其次,在历史时间过后,任何新接收的路由如果其前缀起源与上述提取结果相违背(产生 MOAS),将被视为可疑路由并被隔离一段时间(suspicious period).如果隔离时间过后可疑路由仍然存在路由表中,则可疑路由将被视为合法且被路由器采用.

PGBGP 方案实际上利用了大多数前缀劫持事件持续时间都较短(45%不超过 24 小时[18])这一统计现象,通过使路由器推迟采用可疑路由的办法避开前缀劫持的威胁时间段,从而免受劫持事件带来的影响.该方案存在的一个重要问题是如何确定历史时间和隔离时间两个参数,以避免误报或漏报.

4.2.2 主动探测技术

主动探测技术从数据平面反馈的信息来印证前缀劫持的发生.主动探测技术一般需要设立若干观测点(vantage point),从观测点发出探测数据包,然后分析响应数据包,提取相关特征信息以鉴别劫持事件的发生与否.根据观测点所处网络位置的不同,我们将主动探测技术归纳为以下两类:

(1) 由外向内探测

这一类的探测技术将观测点选择在目标前缀所处自治域的外部,比较典型的是 Zheng 等人[65]提出的一种轻量级分布式前缀劫持检测机制.该机制的建立出于以下两点考虑:

若未发生前缀劫持,则:

A. 从观测点到目标前缀的网络距离应该是稳定的;

B. 选定一个靠近目标前缀的参考点,则从观测点到参考点的网络路径应该是观测点到目标前缀路径的子集(sub-path).

基于上述两个原则,Zheng 等人设计了如下方案:首先,在目标前缀所处自治域外部选取一定数量的观测点,之后,周期性地测量从观测点到目标前缀的网络距离;若检测到网络距离发生显著变化,则进一步测量观测点到参考点路径和到目标前缀路径的一致性;若存在显著的不一致,则判定该目标前缀已被劫持.

(2) 由内及外探测

这一类探测技术的观测点位于目标前缀所处自治域的内部,代表方案是 Zhang 等人提出的 ISPY[66].该方案利用了本节前面分析的前缀劫持的数据平面特征:源地址为被劫持地址的数据包可能有去无回.也就是说,前缀劫持使部分 AS 受到污染,从前缀合法所有者向这些被污染的 AS 发出探测数据包时会遭遇失败,因为响应数据包可能在返回途中被路由到劫持者的网络中去.这种特征表现在 AS 这一层次上,就是以前缀所有者为中心到

达外部 AS 的可达性视图(view of the reachability)存在很多 cuts.当然,这种 cuts 也可能是因链路中断造成的,但 Zhang 等人的分析表明,前缀劫持所造成的 cuts 远比链路中断造成的 cuts 要多.基于上述原理,该方案成功地实现了以前缀所有者为中心的基于主动探测的前缀劫持检测.

由内及外的探测技术因为只需要在目标前缀所有者中部署,因此更易实施且实时性更好.不足之处是,此类技术需要连续不断地向外发送探测数据包,对自治域本身网络的性能会有所影响.

4.2.3 两者结合

前面的分析表明,MOAS 检测技术可部署性强,适用面广,但时效性差且容易产生误报.主动探测技术能够准确、实时地检测前缀劫持,但盲目地发送过多的探测数据会影响其效率.鉴于此,目前新的研究趋势[67,68]是尝试将两者相结合,首先利用 MOAS 检测技术筛选出可疑的路由,然后针对这些可疑的路由发送主动探测数据包进行验证,最后根据探测结果鉴别前缀劫持.这类技术的系统框架如图 11 所示.

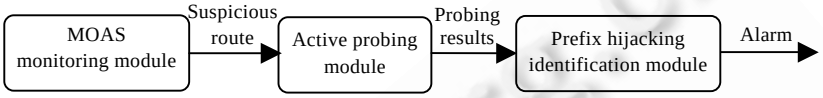



Fig.11 Architecture of MOAS-Probing system

图 11 MOAS-Probing 系统架构

### 4.3 技术比较

路由认证技术和前缀劫持检测技术代表 BGP 安全研究的两大方向,我们对这两类技术作一个综合的比较:

- 路由认证技术以制定和完善 BGP 路由协议的安全机制为目标,利用证书、数字签名和其他加密技术来保护路由信息的真实性和完整性.路由认证技术可以从根本上解决前缀劫持问题,但同时也需要付出不小的代价.这些代价主要包括:需要建立 PKI、路由器的性能开销、需要修改现有协议规范等;
- 前缀劫持检测技术以改善 BGP 安全为目标,基于异常检测(anomaly detection)的概念提取 BGP 控制平面和数据平面的异常信息,对前缀劫持行为进行检测并报警.前缀劫持检测技术不能彻底解决 BGP 的安全问题,但在目前尚未部署完整 PKI 体系的情况下,不失为一种轻量级的解决方案.前缀劫持检测技术不需要修改现有协议规范,但其缺点在于存在误报和漏报的可能.

表 1 列出了这两种技术在各项评价指数上的对比结果.

**Table 1** Comparison of BGP security techniques

**表 1** BGP 安全技术比较

| | 密码技术 | 修改协议规范 | 系统开销 | 实时性 | 轻量级 | 部署难度 |
|---|---|---|---|---|---|---|
| 路由认证技术 | 是 | 是 | 大 | 是 | 否 | 难 |
| 劫持检测技术 | 否 | 否 | 小 | 否 | 是 | 易 |

## 5 未来研究趋势

BGP 安全多年以来一直是一个悬而未解的难题,网络运营商和学术界对此问题始终保持相当的关注.鉴于 BGP 对互联网不可替代的重要性,有关 BGP 路由安全的研究仍将是互联网安全领域的研究热点和重点.我们认为,未来 BGP 安全研究可能集中于以下几个方向:

(1) RPKI & BGPsec 的安全性

RPKI & BGPsec 作为 IETF 着力推广的 BGP 安全标准,其安全性如何还有待深入研究.目前已经有研究发现,RPKI 本身操作的不当会给路由安全带来不利的影响[69].此外,有关 RPKI & BGPsec 标准本身可能存在的安全漏洞也正在讨论[70,71].再者,该标准的增量部署将会导致 BGP 路由交换环境变得混杂,部署了 RPKI &BGPsec 的 AS 与未部署该标准的 AS 同时存在于互联网,这极可能给攻击者以可乘之机,从而给 BGP 安全带来新的未知安全威胁.

(2) 基于 DNS 的 BGP 路由认证

基于 DNS 扩展来验证 BGP 路由的研究[43,72]由来已久,不过一直以来进展不大.随着 ROVER 在将 CIDR 地址编码成反向 DNS 资源记录技术上的突破,基于 DNS 的 BGP 路由认证研究正在重新引起关注,而且由于可以依赖 DNSSEC 来保证认证结果的真实性和完整性,这类技术极有可能成为未来与 RPKI & BGPsec 竞争的 BGP 安全方案.

(3) 基于域间多路径路由的前缀劫持检测

域间多路径路由是 BGP 协议可能的一个发展方向.多路径路由因其最佳路径不再单一,这将使前缀劫持在多路径路由环境下更容易检测出来[73].

(4) 检测和防止路由泄漏

路由泄漏在近期引起了很大的争议和讨论.路由泄漏事件的发生,说明 BGP 安全不仅仅是完善路由认证机制那么简单,如何确保 BGP 路由策略不被违反,也是一个亟需解决的重要的安全问题[13].目前,所有的 BGP 安全技术还无法有效应对路由泄漏,因此,未来非常有必要就如何检测和防止路由泄漏进行深入研究.

## 6 总 结

BGP 协议是互联网关键基础设施的重要组成部分,BGP 安全对于互联网安全起着至关重要的作用.长期以来,BGP 协议因其自身存在的安全漏洞屡屡使互联网遭受严重威胁,研究人员为此提出了各种针对 BGP 安全问题的安全技术和解决方案.这些安全技术部分增强了 BGP 路由协议的安全性,但离彻底解决 BGP 安全问题仍相距甚远.

本文对 BGP 安全研究的过去、现状以及未来进行了全方位的综合阐述,从分析 BGP 协议的设计缺陷着手,讨论由此带来的安全威胁,进而审视用于防御这些安全威胁的现有 BGP 安全机制以及相关的 BGP 安全增强研究.本文期待研究者、运营商以及相关互联网管理机构未来继续努力,使 BGP 安全这一重大课题早日得到完美解决.

**References**:

[1] Rosen EC. Exterior gateway protocol. RFC 827, 1982.

[2] Bono VJ. 7007 explanation and apology. 1997. http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html

[3] Rensys Blog. Internet-Wide catastrophe—Last year. 2005. http://www.renesys.com/blog/2005/12/internetwide_nearcatastrophela.shtml

[4] Rensys Blog. Pakistan hijacks YouTube. 2008. http://www.renesys.com/blog/2008/02/pakistan_hijacks_youtube_1.shtml

[5] BGPmon Blog. How the Internet in Australia went down under. 2012. http://bgpmon.net/blog/?p=554

[6] Pilosov A, Kapela T. Stealing the Internet: An Internet-scale man in the middle attack. Technical Report, Las Vegas: Defcon, 2008. https://www.defcon.org/images/defcon-16/dc16-presentations/defcon-16-pilosov-kapela.pdf

[7] Department of Homeland Security. The national strategy to secure cyberspace. Technical Report, Washington: Department of Homeland Security, 2003. http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf

[8] Kuhn R, Sriram K, Montgomery D. Border gateway protocol security. Technical Report, 800-54, Gaithersburg: NIST, 2007.

[9] Secure BGP project (S-BGP). 2004. http://www.ir.bbn.com/sbgp/

[10] Securing BGP through SecureOrigin BGP. 2006. http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_6-3/securing_bgp_sobgp.html

[11] Secure inter-domain routing (sidr). 2010. http://datatracker.ietf.org/wg/sidr/

[12] Gao L. On inferring autonomous system relationships in the Internet. IEEE/ACM Trans. on Networking, 2001,9(6):733−745. [doi: 10.1109/90.974527]

[13] Huston G. Leaking Routes. The ISP Column, 2012. http://www.potaroo.net/ispcol/2012-03/leaks.html

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

[15] Nordström O, Dovrolis C. Beware of BGP attacks. ACM SIGCOMM Computer Communication Review, 2004,34(2):1−8. [doi: 10.1145/997150.997152].

[16] BGPmon Blog. A BGP leak made in Canada. 2012. http://www.bgpmon.net/a-bgp-leak-made-in-canada/

[17] Rensys Blog. Con-Ed steals the 'net. 2006. http://www.renesys.com/blog/2006/01/coned_steals_the_net.shtml

[18] Mahajan R, Wetherall D, Anderson T. Understanding BGP misconfiguration. In: Proc. of the SIGCOMM 2002. Pittsburgh: ACM Press, 2002. 3−16. [doi: 10.1145/633025.633027]

[19] Zhao X, Pei D, Wang L, Massey D, Mankin A, Wu SF, Zhang L. An analysis of BGP multiple origin AS (MOAS) conflicts. In: Proc. of the SIGCOMM Internet Measurement Workshop. San Francisco: ACM Press, 2001. 31−35. [doi: 10.1145/505203.505207]

[20] BGPmon. http://bgpmon.net/

[21] Cyclops. http://cyclops.cs.ucla.edu/

[22] Dickson B. Route leaks—Definitions. Internet Draft, 2012. http://tools.ietf.org/html/draft-dickson-sidr-route-leak-def-01

[23] Route views project. 2005. http://www.routeviews.org/

[24] Routing information service (RIS). 2011. http://www.ripe.net/data-tools/stats/ris/routing-information-service

[25] Butler K, Farley T, McDaniel P, Rexford J. A survey of BGP security issues and solutions. Proc. of the IEEE, 2010,98(1):100−122. [doi: 10.1109/JPROC.2009.2034031]

[26] Kuzmanovic A, Knightly EW. Low-Rate TCP-targeted denial of service attacks (the shrew vs. the mice and elephants). In: Proc. of the SIGCOMM 2003. Karlsruhe: ACM Press, 2003. 75−86. [doi: 10.1145/863965.863966]

[27] Zhang Y, Mao ZM, Wang J. Low-Rate TCP-targeted DoS attack disrupts Internet routing. In: Proc. of the 14th Annual Network & Distributed System Security Symp. San Diego: The Internet Society, 2007. 1−15. http://www.isoc.org/isoc/conferences/ndss/07/papers/low-rate_TCP-targeted_DOS_attacks.pdf

[28] Schuchard M, Vasserman EY, Mohaisen A. Losing control of the Internet: Using the data plane to attack the control plane. In: Proc. of the 18th Annual Network & Distributed System Security Symp. San Diego: The Internet Society, 2011. http://www.isoc.org/isoc/conferences/ndss/11/pdf/4_1.pdf [doi: 10.1145/1866307.1866411]

[29] Heffernan A. Protection of BGP sessions via the TCP MD5 signature option. RFC 2385, 1998.

[30] Gill V, Heasley J, Meyer D. The generalized TTL security mechanism (GTSM). RFC 3682, 2004.

[31] Wang XY, Yu HB. How to break MD5 and other hash functions. In: Proc. of the 24th Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Aarhus: Springer-Verlag, 2005. 19−35. [doi: 10.1007/11426639_2]

[32] MD5rainbow. http://www.md5rainbow.com/

[33] Villamizar C, Chandra R, Govindan R. BGP route flap damping. RFC 2349, 1998.

[34] Mao ZM, Govindan R, Varghese G, Katz RH. Route flap damping exacerbates Internet routing convergence. In: Proc. of the SIGCOMM 2002. Pittsburgh: ACM Press, 2002. 221−233. [doi: 10.1145/633046.633047]

[35] Smith P, Panigl C. RIPE routing working group recommendations on route-flap damping. Technical Report, ripe-378, Amsterdam: RIPE, 2006.

[36] Caesar M, Rexford J. BGP routing policies in ISP networks. IEEE Network Magazine, 2005,19(6):5−11. [doi: 10.1109/MNET.2005.1541715]

[37] Durand J, Pepelnjak I, Doering G. BGP operations and security. Internet Draft, 2012. http://tools.ietf.org/html/draft-jdurand-bgp-security-01

[38] CIDR report. http://www.cidr-report.org/as2.0/

[39] IRR. http://www.irr.net/index.html

[40] Alaettinoglu C, Villamizar C, Gerich E, Gerich D, Meyer D, Bates T, Karrenberg D, Terpstra M. Routing policy specification language (RPSL). RFC 2622, 1999.

[41] Villamizar C, Alaettinoglu C, Meyer D, Murphy S. Routing policy system security. RFC 2725, 1999.

[42] Liu X, Zhu PD, Peng YX. Internet registry mechanism for preventing prefix hijacks. Ruanjian Xuebao/Journal of Software, 2009,20(3):620−629 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3221.htm [doi: 10.3724/SP.J.1001.2009.03221]

[43] Bates T, Bush R, Li T, Rekhter Y. DNS-Based NLRI origin AS verification in BGP. Internet Draft, 1998. https://tools.ietf.org/html/draft-bates-bgp4-nlri-orig-verif-00

[44] Goodell G, Aiello W, Griffin T, Ioannidis J, McDaniel P, Rubin A. Working around BGP: An incremental approach to improving security and accuracy of interdomain routing. In: Proc. of the 10th Annual Network & Distributed System Security Symp. San Diego: The Internet Society, 2003. http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/5.pdf

[45] Kent S, Lynn C, Seo K. Secure border gateway protocol (S-BGP). IEEE Journal on Selected Areas in Communications, 2000,18(4): 582−592. [doi: 10.1109/49.839934]

[46] Lynn C, Mikkelson J, Seo K. Secure BGP (S-BGP). Internet Draft, 2003. http://tools.ietf.org/html/draft-clynn-s-bgp-protocol-01

[47] Kent S, Lynn C, Mikkelson J, Seo K. Secure border gateway protocol (S-BGP) real world performance and deployment issues. In: Proc. of the Annual Network & Distributed System Security Symp. San Diego: The Internet Society, 2000. http://www.isoc.org/isoc/conferences/ndss/2000/proceedings/045.pdf

[48] White R. Securing BGP through secure origin BGP. Internet Protocol Journal, 2003,6(3):15−22.

[49] Huston G, Rossi M, Armitage G. Securing BGP—A literature survey. IEEE Communications Surveys & Tutorials, 2011,13(2): 199−222. [doi: 10.1109/SURV.2011.041010.00041]

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

[51] Lepinski M. BGPSEC protocol specification. Internet Draft, 2012. https://datatracker.ietf.org/doc/draft-ietf-sidr-bgpsec-protocol/

[52] BGP ROVER: Route origin verification. http://rover.secure64.com/

[53] Gersch J, Massey D, Osterweil E. Reverse DNS naming convention for CIDR address blocks. Internet Draft, 2012. https://datatracker.ietf.org/doc/draft-gersch-dnsop-revdns-cidr/

[54] Gersch J, Massey D, Olschanowsky C. DNS resource records for BGP routing data. Internet Draft, 2012. https://datatracker.ietf.org/doc/draft-gersch-grow-revdns-bgp/

[55] Arends R, Austein R, Larson M, Massey D, Rose S. DNS security introduction and requirements. RFC 4033, 2005.

[56] Le ZJ, Xiong NX, Yang B, Zhou YZ. SC-OA: A secure and efficient scheme for origin authentication of inter-domain routing in cloud computing networks. In: Proc. of the 25th IEEE Int'l Symp. on Parallel and Distributed Processing. Anchorage: IEEE Computer Society, 2011. 243−254. [doi: 10.1109/IPDPS.2011.32]

[57] Hu YC, Perrig A, Sirbu M. SPV: Secure path vector routing for securing BGP. In: Proc. of the SIGCOMM 2004. Portland: ACM Press, 2004. 179−192. [doi: 10.1145/1015467.1015488]

[58] Butler K, McDaniel P, Aiello W. Optimizing BGP security by exploiting path stability. In: Proc. of the 13th ACM Conf. on Computer and Communications Security. Alexandria: ACM Press, 2006. 298−310. [doi: 10.1145/1180405.1180442]

[59] Oorschot PC, Wan T, Kranakis E. On interdomain routing security and pretty secure BGP (psBGP). ACM Trans. on Information and System Security, 2007,10(3):11. [doi: 10.1145/1266977.1266980]

[60] Hu XJ, Zhu PD, Gong ZH. SE-BGP: An approach for BGP security. Ruanjian Xuebao/Journal of Software, 2008,19(1):167−176 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/19/167.htm [doi: 10.3724/SP.J.1001.2008.00167]

[61] Li Q, Xu MW, Wu JP, Zhang XW, Lee P, Xu K. Enhancing the trust of Internet routing with lightweight route attestation. IEEE Trans. on Information Forensics and Security, 2012,7(2):691−703. [doi: 10.1109/TIFS.2011.2177822]

[62] Zhao X, Pei D, Wang L, Massey D, Mankin A, Wu S, Zhang L. Detection of invalid routing announcement in the Internet. In: Proc. of the Int'l Conf. on Dependable Systems and Networks 2002. Bethesda: IEEE Computer Society, 2002. 59−68. [doi: 10.1109/DSN.2002.1028887]

[63] Lad M, Massey D, Pei D, Wu Y, Zhang B, Zhang L. PHAS: A prefix hijack alert system. In: Proc. of the15th USENIX Security Symp. Vancouver: USENIX Press, 2006. 153−166. http://static.usenix.org/events/sec06/tech/full_papers/lad/lad.pdf

[64] Karlin J, Forrest S, Rexford J. Pretty good BGP: Improving BGP by cautiously adopting routes. In Proc. of the 14th IEEE Int'l Conf. on Network Protocols. Santa Barbara: IEEE Computer Society, 2006. 290−299. [doi: 10.1109/ICNP.2006.320179]

[65] Zheng C, Ji L, Pei D, Wang J, Francis P. A light-weight distributed scheme for detecting IP prefix hijacks in real-time. In: Proc. of the SIGCOMM 2007. Kyoto: ACM Press, 2007. 277−288. [doi: 10.1145/1282380.1282412]

[66] Zhang Z, Zhang Y, Hu YC, Mao ZM, Bush R. iSPY: Detecting IP prefix hijacking on my own. ACM/IEEE Trans. on Networking, 2010,18(6):1815−1828. [doi: 10.1109/TNET.2010.2066284]

[67] Hu X, Mao ZM. Accurate real-time identification of IP prefix hijacking. In: Proc. of the IEEE Symp. on Security and Privacy. Oakland: ACM Press, 2007. 3−17. [doi: 10.1109/SP.2007.7]

[68] Xiang Y, Wang Z, Yin X, Wu JP. Argus: An accurate and agile system to detecting IP prefix hijacking. In: Proc. of the 19th IEEE Int'l Conf. on Network Protocols. Vancouver: IEEE Computer Society, 2011: 43−48. [doi: 10.1109/ICNP.2011.6089080]

[69] Wählisch M, Maennel O, Schmidt TC. Towards detecting BGP route hijacking using the RPKI. In: Proc. of the SIGCOMM 2012. Helsinki: ACM Press, 2012. 103−104. [doi: 10.1145/2342356.2342381]

[70] Kent S, Chi A. Threat model for BGP path security. Internet Draft, 2012. https://datatracker.ietf.org/doc/draft-ietf-sidr-bgpsec-threats/

[71] SIDR. A hack for the next generation of rpki-based origin validation. 2012. http://www.ietf.org/mail-archive/web/sidr/current/msg03990.html

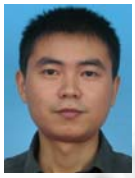
[72] Donnerhacke L, Wijngaards W. DNSSEC protected routing announcements for BGP. Internet Draft, 2008. http://tools.ietf.org/html/draft-donnerhacke-sidr-bgp-verification-dnssec-04

[73] Wang F, Dai B, Su JS. How can multipath dissemination help to detect prefix hijacking. In: Proc. of the 20th Int'l Conf. on Computer Communications and Networks. Maui: IEEE Computer Society, 2011. 1−8. [doi: 10.1109/ICCCN.2011.6005930]

**附中文参考文献:**

[42] 刘欣,朱培栋,彭宇行.防范前缀劫持的互联网注册机制.软件学报,2009,20(3):620−629. http://www.jos.org.cn/1000-9825/3221.htm [doi: 10.3724/SP.J.1001.2009.03221]

[60] 胡湘江,朱培栋,龚正虎.SE-BGP:一种 BGP 安全机制.软件学报,2008,19(1):167−176. http://www.jos.org.cn/1000-9825/19/167.htm [doi: 10.3724/SP.J.1001.2008.00167]



**黎松**(1981－),男,江西高安人,博士生,主要研究领域为计算机网络安全.
E-mail: lisong10@mails.tsinghua.edu.cn

**诸葛建伟**(1980－),男,博士,副研究员,CCF 会员,主要研究领域为网络与系统安全.
E-mail: zhugejw@cernet.edu.cn

**李星**(1956－),男,博士,教授,博士生导师,CCF 高级会员,主要研究领域为通信系统,计算机网络,统计信号处理.
E-mail: xing@cernet.edu.cn