

## BGP 路由泄露研究

贾佳<sup>1,2</sup>, 延志伟<sup>2</sup>, 耿光刚<sup>2</sup>, 金键<sup>1,2</sup>

(1. 中国科学院大学计算机网络信息中心, 北京 100190;

2. 中国互联网络信息中心互联网域名管理技术国家工程实验室, 北京 100190)

**摘要:** 随着互联网规模的急剧扩大, 边界网关协议 (BGP, border gateway protocol) 在域间路由系统中的作用愈加重要。BGP 本身存在很大的安全隐患, 导致前缀劫持、AS\_PATH 劫持及路由泄露攻击事件频频发生, 给互联网造成了严峻的安全威胁。目前, 国内外针对路由泄露的介绍及安全研究机制相对较少。对 BGP 路由泄露进行了详细研究, 介绍了 BGP 内容、路由策略及制定规则, 分析了重大路由泄露安全事件及发生路由泄露的 6 种类型, 并比较了当前针对路由泄露的安全机制和检测方法, 最后对路由泄露安全防范机制提出了新的展望。

**关键词:** BGP; 路由策略; 路由泄露; 路由安全

**中图分类号:** TP393.08

**文献标识码:** A

**doi:** 10.11959/j.issn.2096-109x.2016.00074

## Study on BGP route leak

JIA Jia<sup>1,2</sup>, YAN Zhi-wei<sup>2</sup>, GENG Guang-gang<sup>2</sup>, JIN Jian<sup>1,2</sup>

(1. Computer Network Information Center, University of Chinese Academy of Sciences, Beijing 100190, China;

2. National Engineering Laboratory for Naming and Addressing, China Internet Network Information Center, Beijing 100190, China)

**Abstract:** With the rapid expansion of the scale of Internet, BGP plays a more and more important role in the Inter domain routing system. BGP has a lot of security risks, which result in prefix hijacking, AS\_PATH hijacking and route leak attacks occurring frequently, causing serious threats to the Internet. In currently, the content introduction and security research mechanism were little, so a detailed study of BGP route leak was carried out. The BGP protocol, route policy and established rules were introduced, six types of major route leak security incidents were analysed, the current security mechanisms and methods were summarized and compared to solve and detect route leak. In the last, a new prospect for the security and protection mechanism of route leak was proposed.

**Key words:** BGP, route policy, route leak, route security

### 1 引言

BGP 于 1989 年问世, 作为互联网中最重要  
的域间路由协议, 主要用于不同自治系统 (AS,  
autonomous system) 路由器之间交换路由信息。  
随着互联网规模的急剧扩大, AS 之间的路由选择

愈加复杂, 不同互联网络性能相差很大, 由此考  
虑到路径的使用代价和安全因素, AS 之间的路由  
选择必须要考虑相应路由策略, 选出较优路径。  
所以, BGP 的核心目标是找到一条能够到达目的  
网络并且较优的路由。

然而, BGP 在设计上存在较大的安全缺陷<sup>[1,2]</sup>,

收稿日期: 2016-04-27; 修回日期: 2016-06-06。通信作者: 贾佳, jiajia@cnnic.cn

基金项目: 国家自然科学基金资助项目 (No.61303242)

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

由此导致了許多安全事故。据统计, 主要造成威胁域间路由安全的原因如表 1<sup>[3]</sup>所示。

| 表 1 域间路由问题 |       |
|------------|-------|
| 路由问题       | 百分比/% |
| BGP 错误配置   | 31    |
| 前缀劫持       | 25    |
| 路由泄露       | 22    |
| AS 路径篡改    | 20    |
| 其他         | 2     |

由表 1 可知, 最常见的 BGP 路由安全事件的缘由中 BGP 错误配置比例高达 31%。目前, 针对 BGP 前缀劫持攻击<sup>[4]</sup>和 AS\_PATH 路径劫持攻击<sup>[5]</sup>的安全防御技术研究最为火热, 如 BBN 公司提出的 S-BGP<sup>[6]</sup>、思科公司推出的 soBGP<sup>[7]</sup>以及目前国际互联网工程任务组(IETF, Internet engineering task force)中安全域间路由(SIDR, secure inter-domain routing)工作组正在研究的 RPKI<sup>[8]</sup>与 BGPsec<sup>[9]</sup>技术, 但是以上几种安全机制本身也存在很多安全漏洞和性能缺陷, 至今无法全面部署与实施。同时, 路由泄露对于 BGP 安全有非常重要的影响, 但目前对路由泄露的原因和规避机制研究较少。

本文详细介绍了 BGP 内容、路由策略及其制定规则, 以及发生在 2015 年的重大 BGP 路由泄露安全事件, 并对路由泄露的原因进行了分析。根据分析结果, 本文介绍了目前已提出的路由泄露的定义及 6 种类型, 并对路由泄露的安全机制进行了汇总整理与分析比较。最后本文提出了针对路由泄露安全防范机制的展望。

## 2 BGP 协议概述

### 2.1 BGP 分组介绍

RFC4271<sup>[10]</sup>中规定了 BGP-4 的 4 种分组格式, 分别是 Open 分组、Update 分组、Keepalive

分组及 Notification 分组, 同时在 RFC2918<sup>[11]</sup>中增添了 Route-refresh 分组。几种分组功能介绍如表 2 所示。

上述分组中, Update 分组作用最为重要, 标识了路径属性(AS\_PATH、Local\_pref、Multi\_exit\_disc 等)和网络层可达性信息(NLRI, network layer reachability information)。其中, AS\_PATH 属性表明 Update 分组所经过的 AS 序列。Local\_pref 属性代表本地优先级, 用于告知路由器, 当有多条路径时, 选择优先级最高的路由。Multi\_exit\_disc 属性则是告知外部 AS 到达本地 AS 的最佳路径选择, 即选择 Multi\_exit\_disc 值更小的路由。NLRI 包含一个或一组该路由通告的 IP 地址前缀。当 BGP 路由器接收到新的 Update 分组时, 首先根据路由表选择下一跳 AS, 并在 AS\_PATH 中添加自己所属的 AS 号, 以完成路由通告的转发与传递。

### 2.2 路由策略介绍

BGP 路由器转发路由不仅要根据路由表, 还要参考路由策略。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<sup>[12]</sup>。目前, 路由策略的设定主要取决于 AS\_PATH、Local\_pref 及 Multi\_exit\_disc 路径属性值, 在同等条件下, 优先选择 Local\_pref 值更高、AS\_PATH 路径更短及 Multi\_exit\_disc 值更小的路由为最佳路由。除了上述影响路径性能的属性作为考虑因素之外, 路由策略的制定还要考虑政治、经济及安全等方面的影响。

路由策略的制定通常取决于 AS 之间的关系<sup>[12]</sup>, AS 关系反应了 2 个 BGP 路由器发言人关于商业关系的协议。AS 之间的商业关系大致可以分为 4 种, 如表 3 所示, 分别是 C2P (customer to provider)、P2C (provider to customer)、P2P (peer to peer) 和 S2S (sibling to sibling)<sup>[13]</sup>。Provider AS 为顾客 AS 提供到其他 AS 的传输服务, Peer AS

表 2 BGP 分组功能

| 分组类型             | 作用                                          |
|------------------|---------------------------------------------|
| Open 分组          | 用于 2 个 AS 的 BGP 发言人(即边界路由器)之间构建连通关系, 使通信初始化 |
| Update 分组        | 用来对某一路由信息进行通告, 或者撤销多条路由                     |
| Keepalive 分组     | 保证一段时间内相邻 AS 之间的连通性, AS 之间会周期性互发信息          |
| Notification 分组  | 发送检测到的差错信息                                  |
| Route-refresh 分组 | 请求对等端进行重新通告                                 |

之间则提供各自流量传输到对方网络的服务。所以,出于经济利益的考虑,AS 优先选择来自 Customer AS 的路由,其次是 Peer AS 及 Provider AS。换句话说,大部分网络采用的路由策略规则如下<sup>[14]</sup>。

1) 来自 Customer AS 宣告的路由允许传递给 Customer、Peer 和 Provider。

2) 来自 Peer AS 宣告的路由允许传递给 Customer,不允许通告给其他的 Peer 和 Provider。

3) 来自 Provider AS 宣告的路由允许传递给 Customer,不允许通告给其他的 Peer 和 Provider。

表 3 BGP 路由器商业关系

| 发送方      | 接收方      |
|----------|----------|
| Customer | Provider |
| Provider | Customer |
| Peer     | Peer     |
| Internal | Internal |

### 3 路由泄露事件及类型介绍

#### 3.1 Google 服务器中断安全事件

2015 年 3 月 11 日 10:30 UTC 到 3 月 12 日 09:15 UTC,大量 Google 前缀通告被改变路径,所有路由都经过了 Airtel AS9498,如图 1 所示<sup>[15]</sup>,所有 Update 分组中的 AS\_PATH 属性都包括 9498、17488、15169。发生这种事故的原因是 Google AS15169 的对等端 Hathway AS17488,

将由 Google 发起的前缀信息泄露给 Hathway AS17488 的服务提供者 Airtel AS9498。同时 Airtel AS9498 也与许多其他的互联网服务交换中心相连,导致大量的路由被重新选择与通告。

AS15169 与 AS17488 是 Peering 关系,AS9498 是 AS17488 的 Provider,即 AS9498 为 AS17488 提供服务。假设 AS1000 与 AS15169、AS9498 分别是 P2P 与 P2C 关系,路由泄露发生之前,AS1000 选择其他路径达到 AS15169,当 AS1000 发现到达某前缀可以通过 Customer 端,AS1000 则会考虑最佳经济效益,优先选择 AS9498 并且会重新通告路由,导致目标网络不可达。Google 是最大的互联网网站,平均每天处理数 10 亿的终端用户,长时间的不可访问会造成极大的经济损失,甚至对整个互联网产生严重影响。

#### 3.2 路由泄露类型

路由泄露是 BGP 路由系统存在的系统漏洞导致的安全问题,据调查<sup>[16]</sup>,每天都会检测出路由泄露安全事件的发生,轻则导致网络不可达,重则可能会导致整个互联网瘫痪。根据对已发生的路由泄露安全事件的观察分析,可以将其分为 6 种类型<sup>[17]</sup>。

如图 2 所示,假设有 6 个自治系统,分别从 AS1~AS6。多宿主 AS3 分别为 AS1 和 AS2 的 Customer,AS2 为 AS6 的 Customer,其余 AS1、AS2、AS5 为 Peering 关系,AS3 与 AS4 为 Peering 关系。具体 6 种路由泄露类型如下。

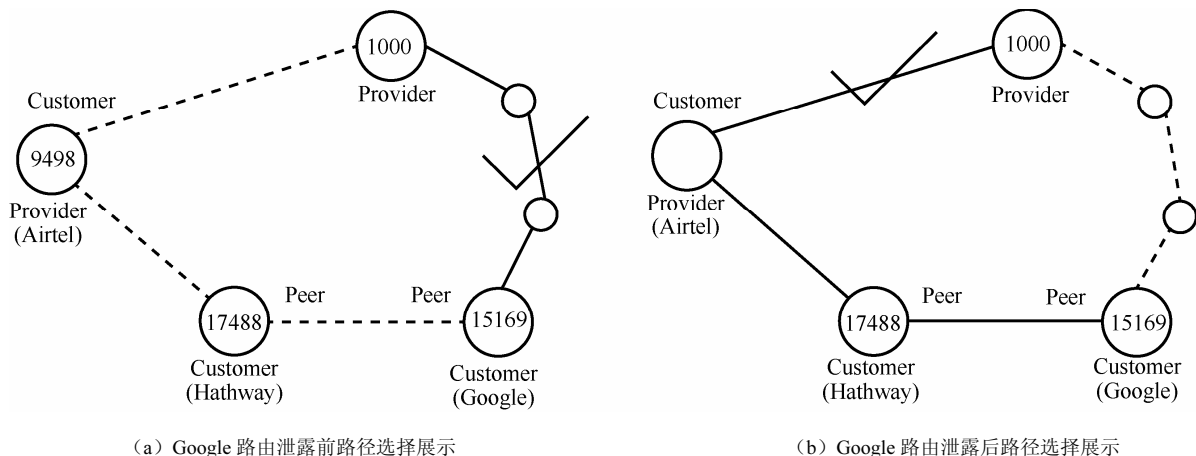


图 1 Google 服务器中断展示

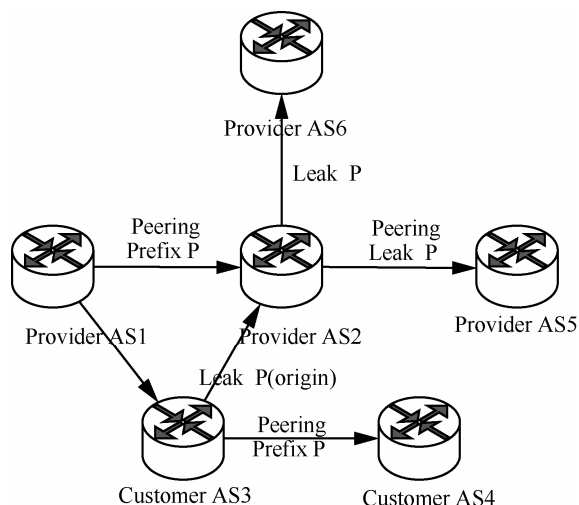


图2 路由泄露

1) AS1 向 AS3 宣告前缀 P 的路由, AS3 将此路由信息泄露给 AS2。

2) AS1 向 AS2 宣告前缀 P 的路由, AS2 将此路由信息泄露给 AS5。

3) AS1 向 AS3 宣告前缀 P 的路由, AS3 将此路由信息泄露给 AS4。

4) AS1 向 AS2 宣告前缀 P 的路由, AS2 将此路由信息泄露给 AS6。

5) AS1 向 AS3 宣告前缀 P 的路由, AS3 作为路由源向 AS2 宣告 P 的路由信息, 改变路径信息。

6) AS 将其内部不可通告前缀或更长前缀路由通告给其他 AS。

综上所述, 来自 Provider 和 Peer 的路由通告只能传播给其 Customer, 否则就会造成路由泄露。

## 4 路由泄露安全机制

### 4.1 前缀过滤及路径过滤机制

前缀过滤<sup>[18,19]</sup>是保护 BGP 路由器免受恶意或非恶意攻击最基本的安全机制, 包括出站前缀过滤和入站前缀过滤。前缀过滤可类比为防火墙, 不允许违背合法规则的前缀通过。AS 可以获知其 Customer AS 与 Peer AS 的通告前缀, 并将其作为过滤前缀的一部分, 不允许不符合条件的 IP 前缀入站或出站。同时对于通信双方, 发送方 AS 的出站过滤器规则要与对等端 AS 的入站过滤器规则相匹配。如图 3 所示, AS1 出站过滤器设定规则为出站前缀属于前缀集合 P, 对于 AS1 的

BGP 对等端, AS2 则建立入站过滤器, 确保经过入站过滤器后的前缀仍属于 P。上述过滤操作可以有效防止攻击者在传递中对前缀信息进行伪造或者更改等恶意操作。

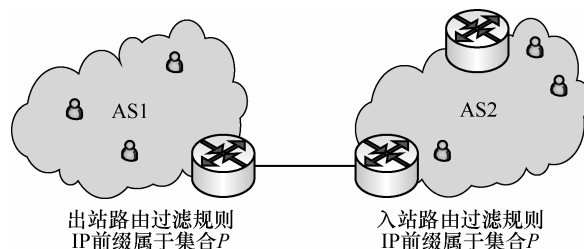


图3 前缀过滤规则实例

除上述设计规则外, 还有一些其他需要考虑的规则。

1) 拒绝现在或者将来用于特殊用途的前缀<sup>[20]</sup>通过。

2) 拒绝未被分配使用的前缀通过。

3) 拒绝拥有不符合条件的前缀长度的前缀通过。

4) 尽可能合并聚合路由。

5) 拒绝内部网络的 IP 地址通过等。

但是, 对于 ISP 来说, 构建 Customer AS 集合的前缀过滤器非常困难, 尤其是 Customer 集合中包含更多的层次划分。而且 ISP 需要定期对过滤器进行维护、保持过滤规则的正确性、保证过滤器中前缀的时效性和正确性等, 这些要求对于规模庞大的 ISP 看来, 具有极大的挑战性。所以, 前缀过滤机制针对防范路由泄露只能起到辅助互补作用, 无法全面保证其安全性与正确性。

路径过滤机制<sup>[21]</sup>则是利用观测到的所有 Customer AS 和 AS Path, 构造 AS Path 路径过滤规则, 防止其他 AS 重新宣告已存在路径的路由。针对 AS Path 的路径过滤机制比前缀过滤机制具有轻量级的优势, 减少对路由器的性能负载。

但是, AS 之间不同会话可能代表着不同的关系模型, 所以, 基于 AS Path 路径过滤的方法会限制 AS 之间正常路由的传递, 而且对 AS Path 过滤器参数的设置错误仍可能会导致路由泄露的发生。

## 4.2 路由注册表过滤机制

利用互联网路由注册<sup>[22]</sup> (IRR, Internet routing registries) 信息和路由策略规范语言<sup>[23,24]</sup> (RPSL, routing policy specification language) 对人工管理进行路由过滤是一种理论上可行的方法。

IRR 是一个开源的分布式数据库, 提供了一种验证 BGP 宣告信息内容正确性的机制。RPSL 是一种丰富的规范语言, 允许用户根据与相邻 AS 关系和传递策略描述出该网络的输入、输出策略。针对上述特性, AS 可以利用 IRR 和 RPSL 构造出所有相邻网络的前缀和 AS 路径的过滤集合, 用来过滤非法路由。早期阶段, 出现了很多尝试利用路由注册信息准确过滤的工具。

但此种方法在实际应用中面临很大的问题, 注册路由表数量庞大, 全部加载到路由器会造成路由器很大的性能负载, 而且 IRR 缺乏监管机制, 无法保证其绝对完整性与正确性, 甚至可能包含冲突信息。目前, 很多地区的互联网运营商不再使用路由注册的方式, 而是采用自己定制的一些工具, 所以, 采用这种方式防范泄露和攻击存在很大的安全风险。

## 4.3 RPKI&BGPsec

RPKI&BGPsec<sup>[25]</sup>是当前 IETF SIDR 工作组主推的 BGP 安全防范机制, 主要针对前缀劫持攻击和 AS\_PATH 路径劫持攻击 2 种攻击形式。根据已有研究<sup>[26]</sup>, RPKI&BGPsec 可以有效解决上述路由泄露攻击类型中 5、6 这 2 种攻击类型。

类型 5 介绍了 Customer AS 将从其 Provider AS 得到的 IP 前缀据为己有, 作为路由源重新向另一个 Provider AS 通告这个路由前缀。另一个 Provider AS 一旦部署了 RPKI, 当接收到篡改路由源的路由时, 首先检查合法的路由源授权 (ROA, route origin authorization) 过滤表, 此时路由源 AS 与 IP 前缀不匹配, 丢弃分组, 类型 5 路由泄露攻击失败。如图 4 所示, AS2 将自己作为前缀 P 的路由源向其 Provider AS3 重新通告, AS3 收到路由后检测 ROA 过滤表, 发现前缀 P 由 AS1 合法通告, 所以, 此条路由无效, 继而丢弃路由。

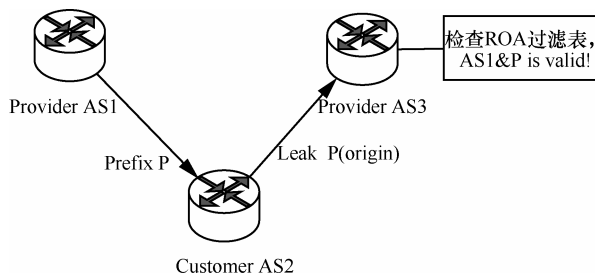


图4 RPKI 防范路由泄露

类型 6 则是典型的 AS 内部前缀泄露, 这些前缀不允许被通告到互联网中。如图 5 所示, 这种情况下, 接收方 AS 可以利用 ROA 将其进行过滤。因为这些前缀没有对应的 ROA 授权或者有专门的特殊 ROA 过滤表。

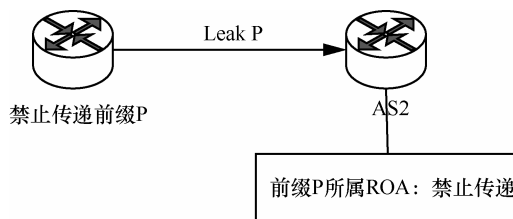


图5 防范内部前缀（禁止传递）IP 展示

当 AS 泄露了其更详细的前缀时, 如图 6 所示, ROA 过滤表包含短前缀的 IP 地址, 根据 RPKI 制定规则<sup>[27]</sup>, 路由将被标识为无效, 类型 6 路由泄露攻击失败。

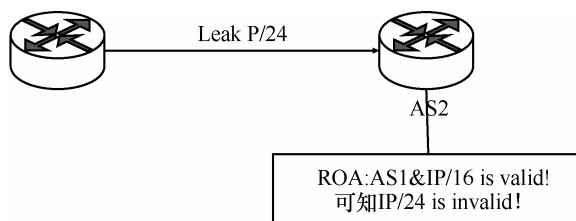


图6 防范内部前缀（长前缀）IP 展示

然而, RPKI&BGPsec 无法防范前 4 种针对路由策略和 AS 关系的路由泄露类型, 所以, 为了更好地加固 BGP 安全机制, 需要在不影响现有功能和性能的前提下, 对 RPKI&BGPsec 进行安全功能扩展。

## 4.4 RLP 保护机制

路由泄露保护 (RLP, route-leak protection) 机制<sup>[26]</sup>是在每一跳的 Update 分组中添加一个新的字段, 即 RLP 字段, 以待接收端路由器检测 AS\_PATH 中是否存在不应该转发的路由证明。

为了检测和缓解路由泄露的问题, RLP 字段值有 2 种选择: 一种是 00, 表示默认的选择, 即不受任何限制; 另一种是 01, 表明不允许向上游 AS 及 (不可传递) Peer AS 转发。目前有 2 种情景可以设置为 01, 即发送 Update 分组给其 Customer AS 或者其 (不可传递) Peer AS。同时, 为了保证区别处于不同商业模式中相同的前缀通告分组, RLP 字段为每一个前缀和每一个邻居 AS 做标注。

当接收端路由器接收到 Update 分组时, 首先检测此分组是否来自其 Customer 或者 (不可传递) Peer AS, 其次检测 Update 中的 RLP 字段是否存在 01 值。如果存在, 则表明 AS\_PATH 中有一跳或者多跳发生了路由泄露。一旦发生了上述情况, 路由器就将此条路由标记为“路由泄露”, 从而优先选择其他安全路由。如果不存在其他未标记的可用路由, 此条标记路由也可能被选择并继续转发。接收端路由器的上述操作可以有效检测和缓解路由泄露的发生。

然而, RLP 保护机制也存在安全隐患。在很大情况下, 一个泄露的路由器可能由于错误配置导致路由标记错误, 并且 RLP 字段没有任何加密机制, 无法保证在传播过程中不会被恶意攻击者篡改或者存在错误配置的可能。所以, 基于这种情况的考虑, RLP 保护机制可以应用到 BGPsec 安全模式中, 作为签名属性的一部分进行逐跳传递与验证。但 BGPsec 机制目前存在较大的性能问题, 对于全面部署的目标还有很长的距离, 而且将 RLP 字段添加到 BGPsec 属性中, 无疑会导致 BGPsec 分组增大并加重路由器的运行负载。

#### 4.5 BGP 角色确认机制

BGP 角色确认机制<sup>[28]</sup>是利用 BGP 角色来表示双方商业关系, 以待第三方进行路由泄露检测。具体来说, BGP 路由器双方在建立连接初始, 即发送 Open 分组时, 对本次通信中双方的商业关系模式达成一致意见。BGP 路由器之间的商业关系可以用 BGP 角色来表示, 并将 BGP 路由器之间的 BGP 角色作为一种新的路径属性进行传递, 作为进行路由决策的配置条件之一。发送方路由器在 Open 分组中向对等端发送各种角色的代号,

如 0 代表未定义、1 代表发送方是 Peer、2 代表发送方是 Provider、3 代表发送方是 Customer、4 代表发送方是 Internal。接收端路由器首先将双方的角色与合法的商业关系规则进行匹配, 如表 3 所示。如果不符合规则, 接收端向发送方发送错误匹配的通知。

BGP Update 分组属性中添加了一项新的属性, 即 OTC (only to customer), 以下 4 种情况, 需要对 OTC 属性进行标识。

1) 如果接收端路由器的角色是 Customer 或者 Peer 时, 所有的入站路由都应该添加 OTC 属性。

2) 携带有 OTC 属性的路由禁止通告给 BGP 角色为 Provider 和 Peer 的对等端。

3) 如果 BGP 双方在发送 Open 分组阶段没有发送 BGP 角色字段及未对双方关系达成一致意见, 并且发送方的角色是 Provider 或者 Peer 时, OTC 属性应该被添加到接收端所有的出站路由中。

4) 当接收端路由器角色是 Provider 或者 Peer 时, 携带 OTC 属性的入站路由应该删除或者优先级降低。

以上 4 种情况可以有效避免路由泄露的生成或者对路由泄露的发生进行检测。后 2 种需要 AS\_PATH 路径中的其他 AS 对路由泄露进行判断。

然而, OTC 作为路径属性可能在传播中被篡改或配置错误, 所以, 也可以与 BGPsec 机制结合, 加密的传递环境可以保证其安全性。

#### 4.6 其他

Geoff Huston 从不同解决问题的视角提出了 2 种方法<sup>[14]</sup>: 一种是利用数据签名、RPKI 及路由注册表共同解决, 但是由此导致系统更加庞大、问题更加复杂; 另一种是从利用分布式算法解答联立方程式的角度出发, 方程式分别代表不同的路由策略, 算法的最终目的是解决单个方程式及全网连通性的问题, 从不同的角度看待路由策略和路由协议交互的方式。

### 5 未来研究趋势

前文提到的几种安全机制, 在 BGP 路由泄露

检测与防范方面都存在缺陷与问题。前缀过滤机制、路径过滤机制及基于路由注册表的过滤机制等过滤方法,无法保证过滤表的时效性和正确性。RLP 保护机制及 BGP 角色确认机制这种在分组中增添安全属性,以待第三方验证的方法无法保证传递信息不被篡改,并且可能会出现错误配置的可能。

路由泄露的发生主要是由于路由器有意或者无意地违背了路由策略。对于路由泄露的安全防范机制可以从如下 2 个方面进行扩展和分析。

1) 过滤机制作为最基本的安全保障机制不可缺省,但未来的发展目标是保证其覆盖范围全面化且过滤规则简单化,不可造成路由器负载重,过滤效果差的结果。

2) 添加新的安全字段标识路由泄露,利用下一跳或者每一跳路由器进行验证的方法较过滤机制更能保障 BGP 安全,但这种安全机制需要与有效的加密方式相结合,才可以确保安全标识的可信度。

由此看来,目前最佳的解决方式是对 RPKI&BGPsec 进行功能扩展,在 BGPsec 的属性中添加标识 AS 关系或者传递属性的字段。同时,BGPsec 机制也面临规模庞大、性能负载重的困境,所以解决 BGPsec 存在的问题也不可忽视。

## 6 结束语

BGP 是当前互联网中唯一的域间路由协议,对互联网安全起着至关重要的作用。然而,BGP 协议本身存在很大的安全问题,导致前缀劫持、AS\_PATH 路径劫持及路由泄露等攻击形式层出不穷。目前,针对前缀劫持和 AS\_PATH 路径劫持的防范攻击安全机制提出了很多方案,但路由泄露由于其危害程度不如前者,所以针对路由泄露的安全方案仍比较少。然而路由泄露攻击形式占 BGP 安全攻击的 22%左右,且每天都会发生或大或小的路由泄露事件,所以路由泄露的研究对于 BGP 安全具有重大意义。

## 参考文献:

- [1] MURPHY S. BGP security vulnerabilities analysis[EB/OL]. <https://tools.ietf.org/pdf/draft-ietf-idr-bgp-vuln-01.pdf>.
- [2] NORDSTRÖM O, DOVROLIS C. Beware of BGP attacks[J].

- ACM Sigcomm Computer Communication Review, 2004, 34(2): 1-8.
- [3] PHOKEER A. Interdomain routing security: motivation and challenges of RPKI[J]. Timss Technical Report, 2013.
- [4] 刘欣, 刘华富. 互联网前缀劫持攻击研究[J]. 计算机技术与发展, 2015(2): 131-134.
- LIU X, LIU H F. Internet prefix hijack attack research[J]. Computer Technology and Development, 2015 (2): 131-134.
- [5] HUSTON G, BUSS R. Securing BGP with BGPsec[J]. Internet Society Org, 2011, 6(5): 15-22.
- [6] Secure BGP project (S-BGP) [EB/OL]. <http://www.ir.bbn.com/sbgp/>.
- [7] WHITE R. Securing BGP through secure origin BGP (SoBGP)[J]. The Internet Protocol Journal, 2003, 6(3):15-22
- [8] LEPINSKI M, KENT S. An infrastructure to support secure Internet routing[EB/OL]. <https://www.rfc-editor.org/rfc/rfc6480.txt>.
- [9] LEPINSKI M, SRIRAM K. BGPsec protocol specification[EB/OL]. <http://ietfreport.isoc.org/all-ids/draft-ietf-sidr-bgpsec-protocol-15.txt>.
- [10] REKHTER Y, LI T, HARES S. A border gateway protocol 4(BGP-4)[S]. RFC 4271, 2006.
- [11] CHEN E. Route refresh capability for BGP-4[S]. RFC 2918, 2000.
- [12] 黎松, 诸葛建伟, 李星. BGP 安全研究[J]. 软件学报, 2013, 24(1): 121-138.
- LI S, ZHU-GE J W, LI X. BGP security studies[J]. Journal of Software, 2013, 24(1): 121-138.
- [13] GAO L. On inferring autonomous system relationships in the Internet[J]. IEEE/ACM Transaction on Networking, 2001, 9(6): 733-745.
- [14] HUSTON G. Leaking routes-the ISP Column 2012[EB/OL]. <http://www.potaroo.net/ispcol/2012-03/leaks.html>.
- [15] Finding and diagnosing BGP route leaks[EB/OL].<http://blog.thousande.com/finding-and-diagnosing-bgp-route-leaks/>.
- [16] BGP routing leak detection system routing leak detection system[EB/OL].<http://pu ck.nether.net/bgp/eakinfo.cgi>.
- [17] SRIRAM K, MONTGOMERY D, MCPHERSON D, et al. Problem definition and classification of bgp route leaks[S]. RFC 7908, 2016.
- [18] DURAND J, PEPELNJAK I, DOERING G. BGP operations and security[S]. RFC 7454, 2015.
- [19] KUHN R,SRIRAM K,MONTGOMERY D. Border gateway protocol security[EB/OL]. <http://csrc.nist.gov/publications/nistpubs/800-54/SP800-54.pdf>.
- [20] IANA.Special-use IPv4 addresses. RFC 3330[EB/OL]. <https://www.rfc-editor.org/rfc/pdf/rfc3330.txt.pdf>.
- [21] PATEL K, HARES S. Analysis of Existing work for I2NSF[EB/OL]. <https://www.ietf.org/id/draft-ietf-idr-asp-path-orf-11.txt>.
- [22] Overview of the IRR[EB/OL]. <http://www.irr.net/docs/overview.html>.

- [23] ALAETTINOGLU C, VILLAMIZAR C, GERICH E, et al. Routing policy specification language(RPSL)[S]. RFC 2622.
- [24] BLUNK L,DAMAS J,PARENT F, et al. Routing policy specification language next generation(RPSLng)[S]. RFC 4012.
- [25] Secure inter-domain routing (sidr)[EB/OL]. <http://datatracker.ietf.org/wg/sidr/>.
- [26] SRIRAM K, MONTGOMERY D, DICKSON B, et al. Method for detection and mitigation of BGP route leaks[EB/OL]. <http://www.ietf.org/id/draft-ietf-idr-route-leak-detection-mitigation-04.txt>.
- [27] HUSTON G, MICHAELSON G. Validation of route origination using the resource certification public key infrastructure(PKI) and route origin authorization (ROAs)[S]. RFC 6483.
- [28] AZIMOV A, BOGOMAZOV E,BUSH R. Route leak detection and filtering using roles in update and open messages[EB/OL]. <http://www.potaroo.net/ietf/IDREF/draft-ymbk-idr-bgp-open-policy/>.



延志伟(1985-), 男, 山西兴县人, 博士, 中国互联网络信息中心副研究员, 主要研究方向为 IPv6、DNS、BGP 等,



耿光刚(1980-), 男, 山东泰安人, 博士, 中国互联网络信息中心研究员, 主要研究方向为机器学习、对抗性信息检索。

#### 作者简介:



贾佳(1992-), 女, 河北石家庄人, 中国科学院大学硕士生, 主要研究方向为 BGP 安全。



金键(1976-), 男, 湖北十堰人, 博士, 中国互联网络信息中心高级工程师, 主要研究方向为 DNS、大规模分布式数据协同、网络可信与安全等。