# 互联网前缀劫持攻击研究

刘 欣,刘华富
(长沙学院 计算机系,湖南 长沙 410003)

**摘 要**:前缀劫持攻击是互联网 BGP 域间路由系统中的首要安全威胁,至今还无有效解决该问题的方案。以前缀劫持攻击为研究对象,分析了前缀劫持攻击产生的具体原因,展现了该攻击在自治系统内部以及在自治系统之间的表现形式与影响;从前缀劫持攻击的危害程度,分析并划分了前缀劫持攻击的基本形态,讨论了各种前缀劫持攻击的基本特性。分析结果表明,子前缀劫持的危害最严重,确切前缀劫持的影响最复杂,而父前缀劫持最易被发现且危害相对较小。

**关键词**:边界网关协议;自治系统;前缀劫持;最优路由
**中图分类号**:TP393 **文献标识码**:A **文章编号**:1673-629X(2015)02-0131-04
doi:10.3969/j.issn.1673-629X.2015.02.030

# Research on Prefix Hijacking in Internet

LIU Xin,LIU Hua-fu
(Department of Computer,Changsha University,Changsha 410003,China)

**Abstract**:Prefix hijacking is the primary security threat in the Internet's BGP system,and presently there is no effective solution against it. Taking the prefix hijacking as the research object,analyze the causes of producing prefix hijacking,showing the form and influence of attack within the autonomous system and between autonomous systems. From the damage degree of prefix hijacking,analyze and divide the basic form of prefix hijacking,and discuss the basic characteristics of various prefix hijackings. The results show that the sub-prefix hijacking is of the most serious hazards,the exact prefix hijacking's impact is the most complex,while the father prefix hijacking is found most easily and the smallest harm relatively.

**Key words**:BGP;autonomous system;prefix hijacking;best routing

## 0 引 言

众所周知,BGP 协议是构建互联网域间路由系统的事实上标准协议[1]。但 BGP 协议自身没有提供任何安全机制保障互联网域间路由系统的安全,因此,BGP 系统中的路由器(即使这些 BGP 路由器属于不同的网络运营商)必须相信系统中传递的网络层可达消息。从协议安全的角度来看,BGP 协议基于一个隐含的假设:BGP 系统中的所有路由器都是可信任的,以至于可进一步推断,互联网中的所有网络运营商都是可信任的。许多研究工作都关注 BGP 协议的安全问题[2-7]。

随着互联网的商业化飞速发展,大量关键应用在互联网上展开,比如电子商务、电子政务和电子金融等。BGP 协议中的这个简单信任模型与互联网商业化之间的矛盾越来越突出:一方面,BGP 协议的信任模型要求所有网络运营商必须完全相互信任;另一方面,互联网的商业化使得网络运营商之间存在既竞争又合作的复杂商业关系。十多年过去了,BGP 系统的安全问题依然存在;更为严重的是,该问题不仅没有好转的迹象,反而愈演愈烈更加令人担忧。

## 1 相关定义

由于 BGP 路由器不能对接收的 BGP 路由中的前缀源信息进行验证,攻击者可利用 BGP 协议的这个安全缺陷实施前缀劫持攻击。而且,在 BGP 路由系统中,若自治系统 A 中的某 BGP 路由器向外宣告了自治系统 B 合法拥有的网络前缀 $p$ 且该路由在互联网上传播,则称自治系统 A 对自治系统 B 的网络前缀 $p$ 发动了

**收稿日期**:2014-03-16 **修回日期**:2014-06-23 **网络出版时间**:2014-10-27
**基金项目**:国家自然科学基金资助项目(61379117);湖南省教育科研基金项目(湘教通[2014]77 号)
**作者简介**:刘 欣(1978-),男,湖南常德人,博士,讲师,CCF 会员,研究方向为域间路由;刘华富,教授,研究方向为传感器技术和计算机网络技术。
**网络出版地址**:http://www.cnki.net/kcms/detail/61.1450.TP.20141027.1429.002.html

前缀劫持(Prefix Hijacking)攻击,或称,自治系统 B 的网络前缀 $p$ 被自治系统 A 劫持。相应的,可称自治系统 A 为这次前缀劫持的攻击者(Attacker),自治系统 B 则为受害者(Victim)。被劫持的路由往往会在互联网的一定范围内传播,对于接收了该劫持路由的自治系统或 BGP 路由器而言(比如自治系统 C),若其 IP 流量的转发行为也被该劫持路由所控制,就称自治系统 C 为该劫持路由的感染者(Infector),反之,则为该劫持路由的携带者(Carrier)[8]。

这里通过例子进一步解释这几个相关概念。如图 1 所示,其展示了一个仅含四个自治系统(AS100 ~ AS400)的自治系统级网络互连图。在图中,AS200 与 AS300 之间为“对等者 - 对等者”的商业关系,而 AS200 与 AS100(以及 AS300 与 AS400)之间为“提供商-客户”的商业关系[9]。假设 AS100 是网络前缀 10.0.0.0/16 的合法拥有者,它可合法地宣告该网络前缀,而 AS400 则非法地宣告了网络前缀 10.0.0.0/16,这就造成 AS400 对 AS100 的网络前缀 10.0.0.0/16 发动了前缀劫持攻击,其中 AS100 为受害者,AS400 为攻击者。

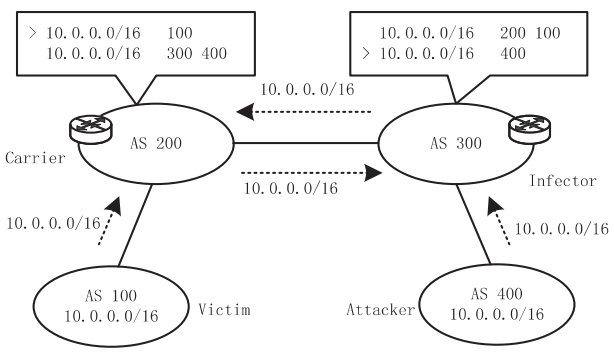


图 1 前缀劫持攻击示例

需注意的是,AS100 宣告的合法路由有可能会通过 AS200 传播至 AS300,与此同时,AS400 宣告的劫持路由也有可能会通过 AS300 传播至 AS200,具体情况详见图 1 中 AS200 与 AS300 中各自的 BGP 路由表。当 AS200 和 AS300 相互交换了各自的 BGP 路由之后,它们都同时得到合法路由与劫持路由,但考虑到自治系统之间的商业关系以及本地路由策略等因素,AS200 会选择合法路由为最优路由,而 AS300 却选择劫持路由为最优路由。这样,尽管 AS200 接收了劫持路由,但是它的 IP 数据转发行为却是正常的,AS200 为劫持路由的携带者;而 AS300 的 IP 数据转发行为则由于受到劫持路由的影响,不能把 IP 数据送到正确的目的地 AS100,所以 AS300 为劫持路由的感染者。

## 2 前缀劫持分类

根据受害者与攻击者所宣告网络前缀之间的关系,可把前缀劫持攻击分为三种基本类型:父前缀劫持、子前缀劫持和确切前缀劫持。

### 2.1 父前缀劫持(Father Prefix Hijacking)

在某前缀劫持事件中,假设受害者合法拥有网络前缀 $p_1$ 包含的 IP 地址空间且宣告的网络前缀为 $p_2$,攻击者宣告的网络前缀为 $p_1$,若网络前缀 $p_2$ 是 $p_1$ 的真子集,即 $p_2 \subset p_1$,就称这次前缀劫持是针对网络前缀 $p_2$ 的父前缀劫持。如图 2 所示,假设 AS100 合法拥有网络前缀 10.0.0.0/8 所包含的 IP 地址空间,但只合法地宣告了网络前缀 10.0.0.0/16,而 AS300 非法宣告了网络前缀 10.0.0.0/8,由于攻击者 AS300 宣告的网络前缀为受害者 AS100 所有且包含受害者所宣告的网络前缀,所以这次前缀劫持事件是父前缀劫持。

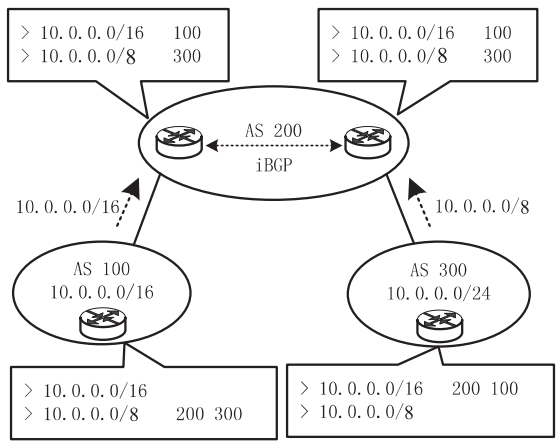


图 2 父前缀劫持攻击示例

父前缀劫持具有两大特点:

(1)父前缀劫持通常有着全局性的影响。劫持路由可污染互联网 DFZ(Default Free Zone)区域内的所有 BGP 路由表,甚至在受害者的 BGP 路由表中也可观察得到。比如,在图 2 中,AS300 非法宣告的前缀 10.0.0.0/8 就出现在网络中所有 BGP 路由器的 BGP 路由表中,特别地,还出现在受害者 AS100 的 BGP 路由表中。从这个角度来看,父前缀劫持比较容易被发现,因为受害者只需观察本自治系统中的 BGP 路由表就可发现这样的前缀劫持。

(2)受到父前缀劫持影响的 BGP 路由器都是劫持路由的携带者,而非感染者。这是由于互联网采用最长前缀匹配规则(Longest Prefix Matching)转发 IP 数据包,因而父前缀劫持往往不会影响互联网到受害者相关网络的 IP 层连通性。比如,尽管攻击者 AS300 非法宣告前缀 10.0.0.0/8 所产生的 BGP 路由被携带者 AS200 的 BGP 路由器选为最优路由,但是在转发 IP 数据包时,真正起作用的路由还是来自受害者 AS100 宣告的合法前缀 10.0.0.0/16 所产生的 BGP 路由。

然而,网络管理员不能因为父前缀劫持的这些特点而对其掉以轻心。首先,父前缀劫持会污染 DFZ 区

域的所有 BGP 路由表,这会带来不必要的通信、存储和处理开销;其次,父前缀劫持就像一颗定时炸弹随时都可能会产生问题,假若受害者 AS100 由于某种原因暂时撤销了网络前缀 10.0.0.0/16,那么攻击者 AS300 非法宣告的前缀 10.0.0.0/8 所产生的 BGP 路由就会控制携带者 AS200 的 IP 数据转发行为;相关研究还指出[10],在实施网络攻击期间,恶意攻击者若能够配合对目标网络进行短暂的父前缀劫持攻击,就可在发送大量的垃圾邮件、发动 DoS 等网络攻击之后不留痕迹,而不会暴露攻击源。

### 2.2　子前缀劫持(Child Prefix Hijacking)

与父前缀劫持的定义相类似,在某前缀劫持事件中,假设受害者合法拥有网络前缀 $p_1$ 包含的 IP 地址空间且宣告的网络前缀为 $p_1$,攻击者宣告的网络前缀为 $p_2$,若网络前缀 $p_2$ 是 $p_1$ 的真子集,即 $p_2 \subset p_1$,就称这次前缀劫持是针对网络前缀 $p_1$ 的子前缀劫持。如图 3 所示,AS100 合法地宣告了网络前缀 10.0.0.0/16,而 AS400 非法宣告了网络前缀 10.0.0.0/24,由于攻击者 AS400 宣告的网络前缀是受害者 AS100 所宣告网络前缀的子前缀,所以这次前缀劫持事件是子前缀劫持。

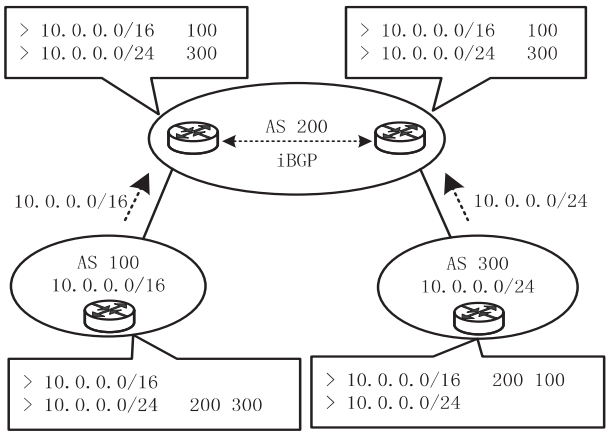


图 3　子前缀劫持攻击示例

由于子前缀劫持会直接影响互联网到受害者网络的连通性,因此危害非常大,主要体现在两个方面:

(1)子前缀劫持的影响范围大,甚至可在受害者的 BGP 路由表中观察到,如图 3 所示。但有一种例外情况需注意,在实际的网络运营中,为限制 BGP 路由表的大小,许多网络运营商会对接收的 BGP 路由的前缀长度有所限制,比如,通常都会要求 BGP 路由中的前缀长度不能大于/24,所以,若攻击者非法宣告过长的前缀就只能影响很小的范围,甚至可能没有影响,但这也导致攻击难以被发现。

(2)受子前缀劫持影响的 BGP 路由器都是劫持路由的感染者,而非携带者。这同样是由于最长前缀匹配规则的作用结果,子前缀劫持会影响互联网到受害者网络的 IP 层连通性。如图 3 所示,由于攻击者 AS300 非法宣告前缀 10.0.0.0/24,感染者 AS200 会把目的地位于前缀 10.0.0.0/24 中的 IP 流量都送往攻击者 AS300,而这些流量本应该是被送往受害者 AS100。

自治系统管理员应时刻关注针对其网络前缀的子前缀劫持事件。子前缀劫持是攻击者的有利武器,除了造成路由黑洞而丢弃流量外,若在实施子前缀劫持攻击的同时,伪造目标网络中的关键站点(比如政府门户网站、金融服务网站等),就可实施非常隐蔽的网络钓鱼攻击,而这一切与互联网是否提供了源地址安全转发服务或安全的 DNS 服务都无关;更为严重的是,若攻击者对 DNS 系统根服务器所属的网络实施子前缀攻击,将会直接危及整个互联网的安全。这绝非危言耸听,曾在互联网上发生的 YouTube 事件就是子前缀劫持事件的典型代表[11]。基于宗教方面的因素考虑,2008 年 2 月 24 日巴基斯坦电信管理局下令禁止在其国内访问 YouTube 网站,巴基斯坦电信(AS17557)采取的技术手段就是非法宣告网络前缀 208.65.153.0/24 以让该网络在巴基斯坦国内不可访问。不幸的是,这些伪造路由意外通过香港的电讯盈科(AS3491)在 BGP 路由系统的 DFZ 区域扩散,最终致使全世界在两个多小时内不能正常访问 YouTube 网站。

### 2.3　确切前缀劫持(Exact Prefix Hijacking)

在某前缀劫持事件中,假设受害者合法拥有网络前缀 $p$ 包含的 IP 地址空间且宣告的网络前缀为 $p$,攻击者宣告的网络前缀也为 $p$,就称这次前缀劫持是针对网络前缀 $p$ 的确切前缀劫持。如图 4 所示,AS100 合法地宣告了网络前缀 10.0.0.0/16,而 AS400 非法宣告了相同的网络前缀 10.0.0.0/16,由于攻击者宣告的网络前缀与受害者所宣告的网络前缀相同,所以这次前缀劫持事件是确切前缀劫持。

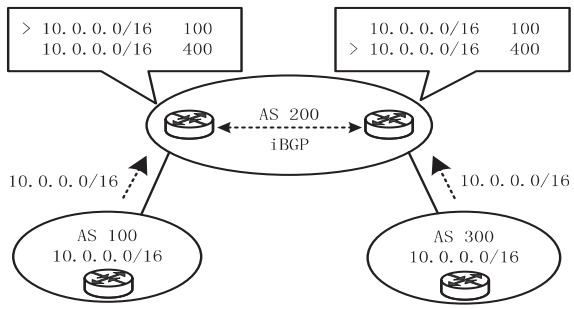


图 4　确切前缀劫持攻击示例

与前两种前缀劫持攻击相比,确切前缀劫持最大的特点就是它的表现行为相对较复杂,因而难以被发现。由于受害者与攻击者宣告了相同的前缀,它们在 BGP 路由系统中传播时会相互竞争、相互影响,而不会像子(或父)前缀劫持那样只表现出单一性质的全局

影响特性。一般而言,确切前缀劫持在 BGP 路由系统中的影响范围不确定,不仅受到攻击者和受害者在互联网中所处的位置影响,而且还受到每一中转自治系统本地路由策略的影响[12]。回顾图 1,该图实际上展示了一个确切前缀劫持的例子,其中 AS200 和 AS300 同时都学到了合法路由与劫持路由,但由于各自本地路由策略的原因,它们对劫持路由采取了不同的态度,因而受确切前缀劫持的影响各不相同:AS200 优选了合法路由而成为携带者,而 AS300 优选了劫持路由而成为感染者。

确切前缀劫持的复杂性还表现在,即使是在一致路由策略的单自治系统中,确切前缀劫持对其内部不同 BGP 路由器也会产生不同影响,图 4 就展示了这样的一个例子。在图 4 中,AS200 中的两台 BGP 路由器都学到了劫持路由和合法路由,但它们对劫持路由采取了不同的态度。这主要是由于 BGP 路由选择过程的规则所致:若两条 BGP 路由的 WEIGHT、LOCAL_PREF、AS_PATH、Origin、MED 等路由属性都不能确定哪条路由最优的话,那么来自 eBGP 会话的路由要优于来自 iBGP 会话的路由(Prefer eBGP over iBGP paths)[13]。因而,AS200 中左边的 BGP 路由器优选来自 eBGP 会话的合法路由而成为劫持路由的携带者;AS200 右边的 BGP 路由器则相反,它优选来自 eBGP 会话的劫持路由而成为感染者。

此外,MOAS(Multi-Origin AS)冲突现象与确切前缀劫持有关。在当前的 BGP 路由系统中,一个网络前缀通常只能被一个自治系统合法地宣告,而 Zhao 等人发现[14],在互联网骨干 BGP 路由器中存在着许多 MOAS 冲突的现象,即某个网络前缀会同时被多个自治系统宣告。他们进一步指出,MOAS 冲突存在有效与无效之分:有效的 MOAS 冲突是由于合理的网络运营实践产生,比如各种形式的多宿主互连策略、网络交换点 IXP 的网络前缀或任播前缀(anycast prefix)都有可能会被多个自治系统在 BGP 路由系统中宣告;而无效的 MOAS 冲突正是由确切前缀劫持攻击所带来的一种伴随现象。

## 3 前缀劫持比较

在前面的讨论中,可看到不同类型的前缀劫持在影响范围、危害程度以及被发现的难易程度等方面都有差异。还值得注意的是,在当前的互联网域间路由环境中,所有类型的前缀劫持都易于发生,但也都非常难于防范和恢复,至今依然缺乏实际有效的解决办法。

表 1 对三类前缀劫持的特点进行了总结。相比较而言,由于确切前缀劫持可能会给互联网的不同部分带来不同的影响和危害,人们通常难于发现并诊断这类网络故障,子前缀劫持和确切前缀劫持的危害更大,特别是确切前缀劫持最令自治系统管理员头痛。

表 1 不同类型的前缀劫持比较

| 攻击类型 | 影响范围 | 危害 | 防范 | 检测 | 恢复 |
|---|---|---|---|---|---|
| 父前缀劫持 | 互联网全局 | 较轻,一般不影响网络连通性 | 困难 | 容易 | 困难,需攻击者主动撤销 |
| 子前缀劫持 | 互联网全局 | 非常严重,影响网络连通性 | 困难 | 容易 | 困难,需攻击者主动撤销 |
| 确切前缀劫持 | 互联网局部 | 严重,影响网络连通性 | 困难 | 困难 | 困难,需攻击者主动撤销 |

实际情况中的前缀劫持事件会更加复杂。攻击者宣告的某个网络前缀还可能会与受害者宣告的多个网络前缀之间存在关系,这样的前缀劫持事件是文中所讨论的三种基本攻击的组合;更甚者,随着事态的发展,前缀劫持攻击的类型还可能会由于受害者的自救行为而动态地发生改变。比如,在 YouTube 事件起初,巴基斯坦电信非法宣告了 YouTube 公司的网络前缀 208.65.153.0/24,而 YouTube 公司只宣告了网络前缀 208.65.152.0/22,显然这时的前缀劫持事件是子前缀劫持;但当 YouTube 公司发现该劫持后,作为主动应对措施,它也开始宣告网络前缀 208.65.153.0/24,这时该事件就转变成由确切前缀劫持与子前缀劫持构成的复合前缀劫持事件。

## 4 结束语

文中深入研究了 BGP 路由系统中的前缀劫持攻击。根据伪造路由与合法路由之间的关系将前缀劫持攻击划分为三种基本攻击形态:父前缀劫持、子前缀劫持与确切前缀劫持。讨论了不同类型的前缀劫持攻击在影响范围、危害程度以及被发现的难易程度等方面的特点。考虑到确切前缀劫持攻击的行为十分复杂,下一步工作将针对该类攻击的传播行为、影响范围以及 MOAS 表现特性等方面进行深入研究。

**参考文献:**

[1] 李海华. BGP MPLS VPN 数据转发过程分析[J]. 计算机技术与发展,2011,21(6):4-8.

[2] 徐 恪,熊勇强,吴建平. 边界网关协议 BGP-4 的安全扩展[J]. 电子学报,2002,30(2):271-273.

[3] 胡湘江,朱培栋,龚正虎. SE-BGP:一种 BGP 安全机制[J]. 软件学报,2008,19(1):167-176.

[4] 王 娜,智英建,张建辉,等. 一个基于身份的安全域间路由协议[J]. 软件学报,2009,20(12):3223-3239.

[5] 李 琦,吴建平,徐明伟,等. 自治系统间的安全路由协议 GesBGP[J]. 计算机学报,2009,32(3):506-515.

[6] 刘 欣,朱培栋,彭宇行. Co-Monitor:检测前缀劫持的协

(下转第 139 页)

的值。

(5)通过粒子群算法需找相匹配的数据包。

(6)提取已知数据包的属性,并计算出属性的值。

(7)比较未知数据包的属性与已知数据包的属性的值。

(8)通过属性值的计算和属性值的比较,得出相应的结论。

## 6　结束语

文中提出的新的检测算法是基于现有的入侵检测算法,并首次将粒子群技术应用到入侵检测的异常检测中。这是文中的创新点。异常检测是一种成熟的检测技术,异常检测技术与其他技术相结合的应用前景十分广泛,随着计算机技术和人工智能技术的发展,将会出现更多的新异常检测算法。随着入侵检测技术不断的发展,这必将遏制网络攻击事件的发生,网络攻击事件的成功率将会有明显的下降。

**参考文献:**


[1] 阎　巧,谢维信. 异常检测技术的研究与发展[J]. 西安电子科技大学学报,2002,29(1):128-132.

[2] 金文进,杨　武. 异常检测技术研究综述[J]. 软件导刊,2008,7(1):10-13.

[3] 刘　陶,叶君耀,朱永宣. 一种基于统计方法的入侵检测模型的研究[J]. 微计算机信息,2007,23(10-3):120-122.

[4] 纪祥敏,宁正元,林大辉. 误用检测技术研究[J]. 福建电脑,2006(2):6-7.

[5] Lane T,Brodley C E. Temporal sequence learning and data reduction for anomaly detection[J]. ACM Transactions on Information and System Security,1999,2(3):295-331.

[6] Warrender C,Forrest S,Pearlmutt B. Detecting intrusions using system calls:alternative data mode[C]//Proc of IEEE symposium on security and privacy. Oakland:IEEE,1999:133-145.

[7] Denning D. An intrusion detection model[J]. IEEE Transactions on Software Engineering,1987,13(2):222-232.

[8] 潘　峰,周　倩,李位星,等. 标准粒子群优化算法的马尔科夫链分析[J]. 自动化学报,2013,39(4):381-389.

[9] 高海兵,周　驰,高　亮. 广义粒子群优化模型[J]. 计算机学报,2005,28(12):1980-1987.

[10] 曾建潮,崔志华. 微粒群算法的统一模型及分析[J]. 计算机研究与发展,2006,43(1):96-100.

[11] 刘志雄,梁　华. 粒子群算法中随机数参数的设置与实验分析[J]. 控制理论与应用,2010,27(11):1489-1496.

[12] Eberhart R C,Shi Y. Comparing inertia weights and constriction factors in particle swarm optimization[C]//Proceedings of the IEEE congress on evolutionary computation. [s. l.]:[s. n.],2000:84-88.

[13] 高　鹰,谢胜利. 免疫粒子群优化算法[J]. 计算机工程与应用,2004,40(6):4-6.


(上接第 134 页)


作监测机制[J]. 软件学报,2010,21(10):2584-2598.

[7] 刘志辉,孙　斌,谷利泽,等. 一种防范 BGP 地址前缀劫持的源认证方案[J]. 软件学报,2012,23(7):1908-1923.

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

[9] Dimitropoulos X A,Krioukov D V,Fomenkov M,et al. AS relationships:inference and validation[J]. ACM SIGCOMM Computer Communication Review,2007,37(1):29-40.

[10] Ramachandran A,Feamster N. Understanding the network-level behavior of spammers[J]. ACM SIGCOMM Computer Communication Review,2006,36(4):291-302.

[11] Adhikari V K,Jain S,Zhang Zhili. YouTube traffic dynamics and its interplay with a tier-1 ISP:an ISP perspective[C]//Proceedings of the 10th ACM SIGCOMM conference on Internet measurement. [s. l.]:ACM,2010:431-443.

[12] Lad M,Oliveira R,Zhang B,et al. Understanding resiliency of internet topology against prefix hijack attacks[C]//Proc of 37th annual IEEE/IFIP international conference on dependable systems and networks. Los Angeles:IEEE,2007:368-377.

[13] BGP best path selection algorithm[EB/OL]. 2006. http://www. cisco. com/warp/public/459/25. shtml.

[14] Zhao Xiaoliang,Pei Dan,Wang Lan,et al. An analysis of BGP multiple origin AS (MOAS) conflicts[C]//Proceedings of ACM Internet measurement workshop. San Francisco,CA,USA:ACM,2001:31-35.

# 互联网前缀劫持攻击研究



作者： 刘欣， 刘华富， LIU Xin， LIU Hua-fu
作者单位： 长沙学院 计算机系,湖南 长沙,410003
刊名： 计算机技术与发展 ISTIC
英文刊名： Computer Technology and Development
年，卷(期)： 2015(2)