ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.20, No.3, March 2009, pp.620−629
doi: 10.3724/SP.J.1001.2009.03221

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

防范前缀劫持的互联网注册机制*

刘 欣+, 朱培栋, 彭宇行

(国防科学技术大学 计算机学院,湖南 长沙 410073)

Internet Registry Mechanism for Preventing Prefix Hijacks

LIU Xin+, ZHU Pei-Dong, PENG Yu-Xing

(School of Computer, National University of Defense Technology, Changsha 410073, China)

+ Corresponding author: E-mail: xin.liu@nudt.edu.cn

Liu X, Zhu PD, Peng YX. Internet registry mechanism for preventing prefix hijacks. *Journal of Software*, 2009,20(3):620−629. http://www.jos.org.cn/1000-9825/3221.htm

Abstract: Based on the registering idea of IRR (internet routing registry), the concept of Prefix Policy is proposed, and a new Internet registry mechanism, E-IRR, is presented. E-IRR offers an efficient and defensive method to prevent hijacked routes. In E-IRR, every participant declares its prefix policies, and makes use of the others' registered prefix policies to validate BGP routes. Measures are designed to guarantee the validity of prefix policies, and evaluate its capabilities of security and performance. The major benefits of the method are the balance it reaches between the capability of preventing prefix hijacks and the security mechanism's requirements of practical deployment, the facts that the method lends itself to stepwise deployment and needs not any BGP extension for security. These properties, not shared by alternative approaches, make it an attractive and viable solution to the prefix hijacking problem.

Key words: BGP; inter-domain routing system; prefix hijacking; prefix policy; IRR; internet registry mechanism

摘 要: 借鉴IRR(Internet routing registry)机制中注册路由策略的思想,提出了前缀策略(prefix policy)的概念,并由此设计了一种防范前缀劫持的方法——E-IRR机制.在E-IRR中,参与者发布自己的前缀策略,同时利用其他自治系统已注册的前缀策略验证BGP路由,从而防范前缀劫持.提出了维护前缀策略有效性措施,评估了E-IRR机制的安全能力与性能.方法的主要优势是,其在前缀劫持的防范能力与安全机制的实际部署需求之间达到了一个较好平衡,可增量式地部署,并不需要对BGP协议进行任何安全扩展.现有方案都不同时具备这些特性,它们使得E-IRR有望实际可行地解决前缀劫持问题.

关键词: 边界网关协议;域间路由系统;前缀劫持;前缀策略;互联网路由注册处;互联网注册机制

中图法分类号: TP393 **文献标识码**: A

* Supported by the National High-Tech Research and Development Plan of China under Grant Nos.2006AA01Z213, 2006AA01Z332 (国家高技术研究发展计划(863)); the National Natural Science Foundation of China under Grant Nos.60673169, 60433040 (国家自然科学基金); the Research Foundation for Ph.D. Candidates of National University of Defense Technology of China, 2007 (国防科学技术大学博士研究生创新基金)

Received 2007-04-06; Accepted 2007-10-26

如今的互联网由 25 000 多个自治系统组成,这些自治系统通过边界网关协议(BGP)传递路由信息,以确保它们之间网络的可达性.BGP 协议是事实上的互联网域间路由协议标准[1].然而,如此关键的路由协议却缺乏必要的安全机制,这使得攻击者可以轻易地实施难以防范的前缀劫持攻击[2].

在前缀劫持中,某 BGP 路由器非法宣告其他网络运营商的 IP 地址空间(或称为前缀),却不实际转发目的地址位于该前缀之中的 IP 数据包.非法入侵或错误配置 BGP 路由器都易于形成前缀劫持攻击,这不仅危及被劫持网络的连通性和安全性,而且可能给整个互联网带来严重影响.实际观察表明,互联网中确实经常发生前缀劫持事件,许多大规模网络瘫痪事故都与此有关[3−5].然而,网络运营商要防范这种路由攻击极其困难.Atkinson 等人在研究后指出,任何形式的前缀劫持防范方案都面临着挑战:不存在完整、准确、真实的信息回答“哪个组织有权利宣告哪个地址块”这个基本问题[6].

在当前的互联网中,网络运营商没有实际有效的办法防范前缀劫持攻击,详见第 1 节的相关工作.已提出的完整方案都要求建立关于 IP 地址空间的 PKI 认证体系.长远来看,建立这种体系非常有必要,因为它可以完全保证 IP 地址空间的合法使用.但是建立这样的体系任重道远,在短期或中期内都难以实现.网络运营商需要实际可行的、有效的防范方案.已有的方案或是安全能力不足,或是不实用,它们大多忽视了一个事实:在当前的现实环境中,只有自治系统自己才能快速且准确地判断其宣告的前缀是否被劫持.

由此,借鉴互联网路由注册处(IRR)中策略注册的思想,本文提出了一种防范前缀劫持的新方法——E-IRR 机制.尽管没有提供强类型的安全能力,但该机制可以有效地帮助网络运营商交换并确认 IP 地址空间所有权.本文还提出前缀策略与可宣告前缀集的概念,扩展路由策略规范语言(RPSL)表达前缀策略,确保在较高层面刻画自治系统拥有的地址空间及使用方式,而又不泄露内部私密信息;运营商利用其他自治系统注册的前缀策略可以得到相应的可宣告前缀集,进而利用本文定义的劫持前缀过滤器就能验证并过滤前缀被劫持的路由.E-IRR 机制采用抢占式注册方式确保前缀策略的有效性:直观的,越多的运营商通过 E-IRR 发布前缀策略,就会吸引越多的运营商使用;相反,越多的运营商利用 E-IRR 得到前缀策略,越多的运营商也就乐于发布.由此,前缀策略的可信度会随着使用而不断增加,这与 IRR 中数据可信度不断降低的过程刚好相反.此外,E-IRR 机制不要求扩展 BGP 协议,因而具有很强的实际部署能力.现有的 BGP 安全方案都不同时具备这些优势,E-IRR 机制在前缀劫持的防范能力与安全机制的实际部署需求之间达到了一个较好的平衡,有望实际可行地解决前缀劫持问题.

本文的工作不能取代完整的互联网域间路由安全方案.我们没有考虑 AS_PATH 或其他 BGP 属性的验证问题.特别地,E-IRR 机制不能防范由于篡改 AS_PATH 而形成类似于前缀劫持的路由攻击.网络管理员通过 E-IRR 机制发布的前缀策略也不能取代区域性互联网注册管理机构(RIR)维护的地址分配记录.E-IRR 机制仅面向网络管理员,帮助他们协作地防范前缀劫持攻击.

本文第 1 节介绍相关工作.第 2 节定义 E-IRR 机制中的前缀策略、可宣告前缀集和劫持前缀过滤器,阐述防范前缀劫持的基本思想.第 3 节详述 E-IRR 机制中前缀策略的语法描述、策略分发方式以及有效性措施等内容.第 4 节评估 E-IRR 机制的安全能力和性能.第 5 节讨论相关问题,最后总结全文.

1 相关工作

从是否需要扩展 BGP 协议来看,可防范前缀劫持的方案大致归为两类:一类是 BGP 协议安全扩展方案[7−12],另一类是防护 BGP 安全的应用系统[13−16].前一类方案以 S-BGP[7]和 soBGP[9]为代表,它们利用 PKI 技术可以严格保证 BGP 路由安全,但由于协议开销等问题,运营商普遍难以接受这些方案.为避免 S-BGP 等强类型安全路由协议在实际应用中遇到的困境,近年提出的 Listen-Whisper[10]及 psBGP[11]等机制以降低安全能力为代价,大量削减协议开销.然而,这些方案也未被运营商所接受,至今依然没有一个 BGP 协议安全扩展方案被实际广泛地应用.至于第 2 类方案,目前存在许多这样的应用系统,比如 PHAS,MyASN 和 IRR 等.这类方案的优势在于无须扩展 BGP 协议,具有很强的实际部署能力,但它们保护 BGP 系统的安全能力较差.考虑到互联网中 BGP 路由器的庞大数目,要确保 BGP 系统安全,任何 BGP 协议安全增强机制可能都不实用,而应用系统类安全方案

也许是今后最有希望的一个发展方向[16].本文的工作属于第 2 类方案,从提升应用系统安全能力的角度开展研究.

在实际网络运营中,许多网络管理员利用注册在 IRR 数据库中的路由策略验证 BGP 路由的有效性.但是 IRR 本身存在许多缺陷,不仅难以有效防范前缀劫持,而且面临与 BGP 协议一样的安全威胁[17].首先,多数 IRR 没有实现路由策略系统安全机制(RPSS),维护者可以注册任意信息.这是 IRR 中数据可信度低,或是越来越低的主要原因.其次,运营商不信任 IRR 中的数据,仅用其来验证客户路由,对来自提供商和对等者的路由不加以限制.显然,这样做只是为了防止客户的错误配置(可无意地产生前缀劫持),而不能防范恶意前缀劫持.第三,IRR 也不能完全阻止客户的错误配置,比如某运营商通过 IRR 自动生成 BGP 配置,那它在注册时所犯的任何错误都会被确认为正常.最后,利用 IRR 中路由对象生成的过滤表往往太长,现有的 BGP 路由器不能提供有效支持.

针对 IRR 的不足,人们也提出多种安全方案来保证其中路由对象的有效性[18−20],比如 IETF 提出的 RPSS 机制[18]、APNIC 正在试用的资源证书[19]等.在这方面做得比较好的一个例子是 RIPE 数据库,RIPE NCC 把 Whois 与 IRR 数据库相结合,并实现了 RPSS 机制,因而 RIPE 数据库中的路由对象具有较高的可信度[20].然而,这些方案与 S-BGP 协议相似,都是以强安全性为目标,要求建立两套认证体系分别验证 IP 地址空间和自治系统号的委托/分配过程,最终达到验证 IRR 中路由对象的目的.与已有的这些方案不同,E-IRR 机制既不考虑复杂的网络资源委托/分配过程,也不关心单个前缀,只是要求自治系统自己注册前缀策略,在较高的层面提供前缀所有权信息,并采用抢占式注册方式帮助自治系统自己确保前缀策略的有效性.E-IRR 机制的目标是在实用性和安全能力之间加以折衷,帮助网络管理员协作地确认 IP 地址空间所有权,从而快速、有效地防范前缀劫持攻击.

2 基本思想

本节定义 E-IRR 机制中的 3 个基本概念:前缀策略、可宣告前缀集以及劫持前缀过滤器.阐述 E-IRR 机制防范前缀劫持的基本思想.

2.1 前缀策略

定义 1(前缀策略(prefix policy)). 在本文中,自治系统的前缀策略是指某自治系统拥有的 IP 地址空间,以及对这些 IP 地址空间的使用方式.

前缀策略是防范前缀劫持所需的关键信息,在当前互联网环境中,通常只有自治系统自己才能快速、准确、完整地提供这些信息,E-IRR 机制利用了这一事实.一方面,各自治系统为防范前缀劫持需要交换前缀策略;另一方面,自治系统又不能泄露自己的私密信息,比如 IP 地址空间的详细使用规划等.这就需要在较高层面定义前缀策略,刻画自治系统拥有的地址空间及使用方式,而又不泄露细节.

可令互联网中自治系统的全体为集合 ASN,自治系统 $\chi\in ASN$.通常,自治系统 χ 对某 IP 地址空间存在 3 种拥有方式:独自拥有、共同拥有和不拥有.为简化起见,仅需考虑前两种方式.

① 独自拥有:这是最常见的一种方式.当自治系统 χ 从相关 RIR 或者上级网络运营商得到 IP 地址空间 P 后,该空间就为自治系统 χ 独自拥有.在这种情况下,自治系统 χ 对地址空间 P 可进一步采用多种使用方式.例如,若自治系统 χ 把空间 P 划分为多个互不相交的子空间,那么对其中的任一子空间 p_i 的使用方式可为:1) χ 自己使用 p_i,即把其中的 IP 地址用于主机编号;2) χ 保留 p_i 以备将来使用;3) χ 把 p_i 委托给自己的客户.

② 共同拥有:从 BGP 域间路由的角度来看,当前互联网中存在许多合理情况造成某 IP 地址空间被多个自治系统共同拥有[21].对于这样的地址空间,自治系统不仅要在前缀策略中指出对其拥有类型为“共享”,而且还要列出所有相关的自治系统.实际上,由于这些自治系统不能随意使用其中的 IP 地址,它们并不是真正地拥有“共享”的 IP 地址空间.因而,自治系统不能像独自拥有方式那样,对共同拥有的空间实施各种使用方式.

由此,自治系统 χ 对 RIR 分配给它的地址空间 P 可能使用如下完整的前缀策略:

① 把地址空间 P 平均划分为 4 个互不相交的子空间 p_1,p_2,p_3,p_4,即满足关系 $p_1\cup p_2\cup p_3\cup p_4=P$ 并且 $p_1\cap p_2\cap p_3\cap p_4=\varnothing$;

② 自己使用子空间 p_1 编号主机;子空间 p_2 保留给自己今后使用;

③ 子空间 p_3 和 p_4 分别委托给客户使用(注意,这里不需要指明具体委托给谁).

目前,BGP 路由器配置语言和标准的 RPSL 语言都不能简洁且直接地描述自治系统 χ 对 IP 地址空间 P 的这种使用方式[22].在 E-IRR 机制中,我们需要扩展 RPSL 语言,使其能够描述前缀策略.

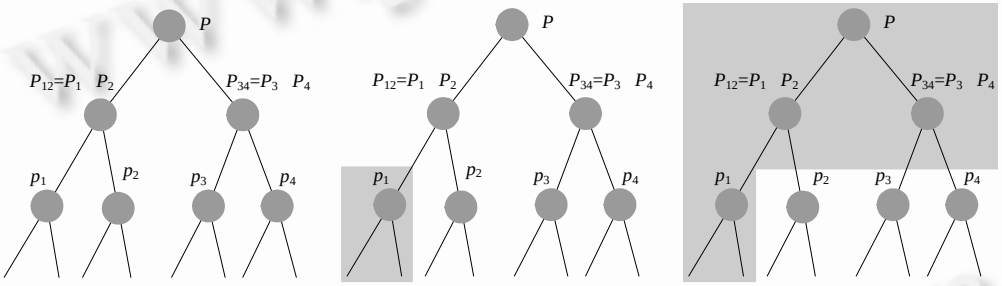
2.2 可宣告前缀集

定义 2(可宣告前缀集(announceable prefix set)). 自治系统的可宣告前缀集是指,根据该自治系统的前缀策略规定,其在公共互联网中可以宣告的前缀集合.比如,自治系统 χ 的可宣告前缀集记为 $A_{SET}(\chi)$,对地址空间 P 的可宣告前缀集可记为 $A_{SET}(\chi,P)$.

通常,我们使用前缀表示法来描述 IP 地址空间.理想情况下,可以把表示 IP 地址空间的所有前缀(记作 *PREFIX*)组织成一棵二叉树,称为前缀树[23].在这棵树中,每个叶节点是只含单个 IP 地址的前缀(或称为 IP 地址),每一非叶子节点有两个子节点(或者,可把子节点称为其父节点的子前缀).图 1(a)展示了自治系统 χ 拥有的 IP 地址空间 P 与子空间 p_1,p_2,p_3,p_4 在前缀树中的关系.其中,前缀 P 的直接子节点为 p_{12},p_{34},它们分别是 p_1,p_2 和 p_3,p_4 的直接父节点.定义前缀 P 的所有子前缀集为 $Prefix_{SET}(P)$,那么前缀 $P,p_{12},p_{34},p_1,p_2,p_3,p_4 \in Prefix_{SET}(P)$.

在前面的规划举例中,自治系统 χ 实际上只使用了子空间 p_1,而没有使用子空间 p_2,p_3,p_4,如图 1(b)中的阴影部分所示.特别要注意的是,自治系统 χ 实际使用的 IP 地址空间与其运营中实际可宣告的前缀之间并非严格的对应关系.比较图 1(b)和图 1(c)的阴影部分可以看到,自治系统 χ 实际可宣告的前缀不仅含有前缀 p_1 的所有子前缀,而且还包含聚合前缀 p_{12},p_{34},P,但是绝不能宣告前缀 p_2,p_3,p_4 中的任何一个子前缀,因为地址空间 p_2 被保留使用,而地址空间 p_3,p_4 被委托给其他网络运营商.由此,就可以得到自治系统 χ 对 IP 地址空间 P 的可宣告前缀集:前缀 p_1 的所有子前缀以及聚合前缀 p_{12},p_{34},P.形式地,该集合可由如下公式计算:

$$A_{SET}(\chi,P)=Prefix_{SET}(P)-Prefix_{SET}(p_2)-Prefix_{SET}(p_3)-Prefix_{SET}(p_4).$$



(a) Prefix tree (a) 前缀树 (b) Used IP address space (b) 已用的 IP 地址空间 (c) Announceable prefix set (c) 可宣告前缀集

Fig.1 Prefix tree and announceable prefix set

图 1 前缀树与可宣告前缀集

自治系统 χ 分别对其拥有的每一个 IP 地址空间定义前缀策略,这些前缀策略规定了自治系统 χ 的全部可宣告前缀 $A_{SET}(\chi)$.假若某自治系统接收到 BGP 路由 r,其前缀属于集合 $A_{SET}(\chi)$,但其来源却不是自治系统 χ,这时,该自治系统就可以马上判定路由 r 为前缀被劫持的伪造路由,因此该路由必须被过滤掉.

2.3 劫持前缀过滤器

过滤器 F 是一个与放置位置无关的函数 $F:PREFIX\times ASN\rightarrow\{0,1\}$,其中 *PREFIX* 和 *ASN* 分别为 IP 地址空间中前缀的全体和互联网中自治系统的全体.可令 BGP 路由 r 的源信息为一个二元关系$\langle prefix,originAS\rangle$,其中,*prefix* 为该路由的网络前缀,*originAS* 为该路由的源自治系统.过滤器 F 就表示,在任何一个自治系统 α 上都可对接收到的 BGP 路由 r 源信息进行检查,以判断该路由是否为前缀被劫持的伪造路由:当 $F(prefix,originAs)=0$ 时为正常;而当 $F(prefix,originAs)=1$ 时,该路由就应该被丢弃.下面给出劫持前缀过滤器的完整定义.

定义 3(劫持前缀过滤器(hijacked prefix filter)). 劫持前缀过滤器为 $F:PREFIX\times ASN\rightarrow\{0,1\}$.对于任意自治

系统α而言,对其接收到源于自治系统χ的 BGP 路由 r,可以使用如下过滤方式:

$$F_\alpha(prefix, originAS)=\begin{cases}0, \text{if } prefix \in A_{SET}(\chi, P) \cap originAS == \chi \\ 1, \text{ otherwise}\end{cases}.$$

由该定义可知,由于过滤器 F 与放置位置无关(但是,过滤器的全局过滤效果与放置位置有关),所有自治系统都可以使用相同的过滤器 F 来防范前缀劫持.显然,过滤器 F 的过滤能力关键在于可以宣告前缀集 A_{SET},而且所有自治系统都应该使用相同的 A_{SET} 集.

值得注意的是,可宣告前缀集 A_{SET} 是为了便于问题的说明和理解而提出来的概念,我们在实际应用中并不需要计算出具体的 A_{SET} 集.因为,从概念上来看,自治系统的可宣告前缀集与其定义的前缀策略在逻辑上是等价的.因此,在后面阐述 E-IRR 机制时,我们通常不加区分地使用这两个概念.

3 E-IRR 机制

3.1 前缀策略描述

为描述自治系统的前缀策略,我们在 RPSL 语言中引入 *route-space* 类及其相关属性,见表 1**.该类中的各种属性根据前面关于前缀策略的讨论来定义,它们的值域和类型域符合标准 RPSL 语言中的基本语法约定,受篇幅限制,这里就不再赘述,细节请参考 RFC-2622.特别要注意的是 *route-space* 类中的 *type* 和 *others* 属性.*type* 属性用于指明其所描述的 *route-space* 对象的类型,值在 *exclusive* 和 *common* 中二取一.当 *type* 的值为 *exclusive* 时,表示 *route-space* 对象只被 *owner* 所指明的自治系统独自拥有;当 *type* 的值为 *common* 时,则表示 *route-space* 对象可以被多个自治系统拥有.这时,*others* 属性必须定义,并且要在值中列出这些自治系统.

Table 1 Definition of the *route-space* class and its attributes

表 1 *Route-Space* 类及其属性的定义

Attribute	Value	Type	Description
route-space	⟨object-name⟩	Mandatory, Single-valued, Class key	Primary key
type	[exclusive| common]	Mandatory, Single-valued	*common* means shared owning, while *exclusive* means exclusive owning
owner	⟨as-number⟩	Mandatory, Single-valued	The owner AS
others	list of ⟨as-number⟩	Optional, Multi-valued	The other related ases
prefix-space	⟨address-prefix⟩	Mandatory, Single-valued	The IP address spaces owned by the owner AS
exclude-space	list of ⟨address-prefix⟩	Optional, Multi-valued	The list of delegated IP address spaces
reserved-space	list of ⟨address-prefix⟩	Optional, Multi-valued	The list of reserved IP address spaces
mnt-by	list of ⟨mntner-name⟩	Mandatory, Multi-valued	The list of maintainer
changed	⟨email-address⟩ ⟨date⟩	Mandatory, Multi-valued	Notification email address

为保证前缀策略语法的有效性,我们定义了 3 个合式规则用以检测网络管理员错误定义的 *route-space* 对象.最基本的,对于一个 *route-space* 对象,其中的强制属性必定不能为空.由此,定义合式规则 1.

合式规则 1.对于任意 *route-space* 对象α,其应该满足:

$$\alpha.route\text{-}space\neq\varnothing\wedge\alpha.type\neq\varnothing\wedge\alpha.owner\neq\varnothing\wedge\alpha.prefix\text{-}space\neq\varnothing.$$

在单个 *route-space* 对象中,若其中定义了可选属性 *exclude-space* 与 *reserved-space*,它们表示的前缀空间必定不能有交集,因为某前缀空间不可能既被自己保留又被分配出去;而且 *exclude-space* 与 *reserved-space* 都应该在 *route-space* 定义的前缀空间中.由此,得到合式规则 2,其定义如下:

合式规则 2.对于任意 *route-space* 对象α,其应该满足以下 3 个条件:

① $Prefix_{SET}(\alpha.exclude\text{-}space)\cap Prefix_{SET}(\alpha.reserved\text{-}space)=\varnothing$;

② $Prefix_{SET}(\alpha.exclude\text{-}space)\subseteq Prefix_{SET}(\alpha.prefix\text{-}space)$;

③ $Prefix_{SET}(\alpha.reserved\text{-}space)\subseteq Prefix_{SET}(\alpha.prefix\text{-}space)$.

** 在 *route-spcae* 类定义中出现的值⟨*XXX*⟩,比如⟨*object-name*⟩和⟨*address-prefix*⟩在 RFC-2622 中定义.

type 属性要求:若 *type* 属性值为 *exclusive* 表示该对象为 *owner* 定义的自治系统所独自使用,这时应该不定义或者忽略掉 *others* 属性;若 *type* 属性值为 *common*,则表示该对象不仅为 *owner* 定义的自治系统所有,而且可为 *others* 属性中的多个自治系统共同使用,那么 *others* 属性必定不能为空.由此,得到合式规则 3.

合式规则 3.对于任意 *route-space* 对象α而言,其应该满足:

$$若\alpha.type=\text{“}common\text{”},则\alpha.others\neq\varnothing.$$

由于 *route-space* 类基于标准的 RPSL 语言规则来进行定义,因此,利用现有 IRR 数据库本身的机制可以保证一定的有效性,比如可以保证合式规则 1,但是 IRR 不能保证合式规则 2 和规则 3.因此,我们要求 E-IRR 数据库能够支持合式规则 1~规则 3,并且,每当网络运营商定义了前缀策略对象之后,最好要首先自己使用合式规则 1~规则 3 进行语法检查,通过之后再利用 E-IRR 机制发布.

3.2 前缀策略分发

借鉴 IRR 中路由策略注册的思想,这里给出了 E-IRR 机制中前缀策略的注册式分发方式,如图 2 所示.在 E-IRR 机制中,主要涉及 3 类基本组件:AS-Server 服务器,E-IRR 数据库和 BGP 路由器.每个参与的自治系统都需要设立一个 AS-Server 服务器,参与者通过 AS-Server 服务器把自己定义的前缀策略上载到 E-IRR 数据库中存储;E-IRR 数据库则集中式地保存所有的前缀策略对象.按照某种方式,每个自治系统通过 AS-Server 服务器从 E-IRR 数据库下载最新的前缀策略信息,进而利用这些信息生成 BGP 路由过滤表.然后,自治系统管理员可以再次通过 AS-Server 服务器把生成的过滤表安装到 BGP 路由器上.当这些边界 BGP 路由器接收到来自邻居的 BGP 更新报文时,利用已有的路由过滤机制就可以验证接收的路由报文,并同时过滤掉那些前缀被劫持的伪造路由,从而达到防范前缀劫持的目的.

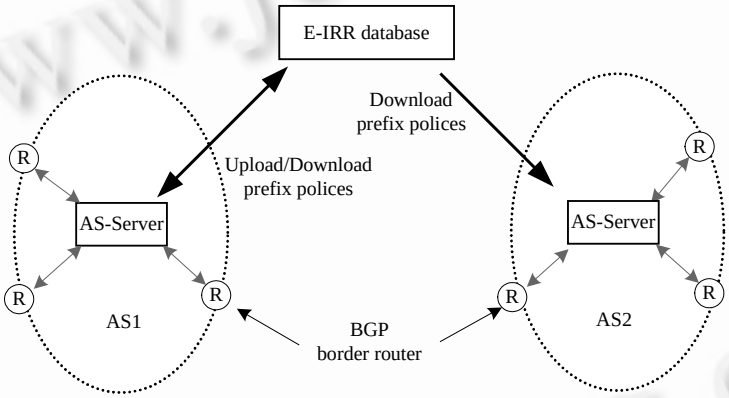


Fig.2 Distributing the registered prefix policies

图 2 前缀策略的注册式分发

注意,在使用 E-IRR 机制时,自治系统管理员可以不发布自己的前缀策略,这正是图 2 中 AS2 的选择.当然,我们不建议加入 E-IRR 的自治系统这样做,因为只有发布了自己的前缀策略才能保护其所拥有的 IP 地址空间.

3.3 有效性措施

在 E-IRR 机制中,若某自治系统要保护自己的前缀不被劫持,则必须在 E-IRR 数据库中正确注册自己的前缀策略;另一方面,若某恶意自治系统要进行前缀劫持攻击,则必须在 E-IRR 数据库中发布伪造的前缀策略.至此,双方关注的焦点都落在 E-IRR 数据库中的前缀策略上.针对这一问题,我们采取的策略是:提供一种机制让网络运营商自己来相互认可 IP 地址空间的所有权,有效性一旦被确定,该机制要能保证以后都不必进行同样的确认.我们首先给出前缀策略的有效性规则,然后介绍抢占式注册方式.

在 *route-space* 类的定义中,为保证共同拥有类型的前缀策略的有效性,我们把 *route-space* 对象定义为 *exclusive* 和 *common* 两种类型:当定义的对象为 *exclusive* 类型时,那么其定义的地址空间必定是独有的;相反,当

多个 *route-space* 对象定义的前缀空间重叠时,这些 *route-space* 对象的类型必须是 *common*;否则,这些前缀策略就产生了冲突.由此,得到检测前缀策略对象冲突的有效性规则.

有效性规则 1.对于 E-IRR 中的任意两个 *route-space* 对象α与β,其应该满足:

若$\alpha.type$="*exclusive*"$\wedge\beta.type$="*exclusive*",

则 $Prefix_{SET}(\alpha.prefix\text{-}space)$-$Prefix_{SET}(\alpha.exclude\text{-}space)$

$\cap Prefix_{SET}(\beta.prefix\text{-}space)$-$Prefix_{SET}(\beta.exclude\text{-}space)=\varnothing$.

有效性规则 2.对于 E-IRR 中的任意两个 *route-space* 对象α与β,其应该满足:

若 $Prefix_{SET}(\alpha.prefix\text{-}space)$-$Prefix_{SET}(\alpha.exclude\text{-}space)$

$\cap Prefix_{SET}(\beta.prefix\text{-}space)$-$Prefix_{SET}(\beta.exclude\text{-}space)\neq\varnothing$,

则$\alpha.type$="*common*"$\wedge\beta.type$="*common*"$\wedge a.owner\in\beta.others\wedge\beta.owner\in a.others$.

在 E-IRR 中,需要对所有 *route-space* 对象进行有效性规则 1 和规则 2 检测,复杂度为 $O(n^2)$.检测算法如下所示,当算法 1 返回的 *RS-Set* 为空时,对象集是有效的;否则,*RS-Set* 中返回冲突的策略对象.

算法 1. 检测 *route-space* 对象集中的有效性.

输入:待检测的 *route-space* 对象集,表示为 *RS*.

输出:策略不一致的 *route-space* 对象对集,表示为 *RS-Set*.

1) 把 *RS* 中的所有元素放到线形表 *list* 中
2) 对于 *list* 中的每一个元素α
3) 把α从 *list* 中移出
4) 对于 *list* 中的每一个元素β
5) 若α与β不满足有效性规则 1 和规则 2
6) 则把$\langle\alpha,\beta\rangle$加入 *RS-Set*
7) 返回结果集 *RS-Set*.

可以假设 E-IRR 中的已有对象集都是有效的,这极大地减少了检测前缀策略对象集有效性的开销.该算法如下所示,其时间复杂度为 $O(n)$.该样的做法是合理的,不但可以大量减少有效性检测的开销;而且,只要保证每次要加入的前缀策略对象与已有对象集是相容的,则 E-IRR 中新的前缀策略对象集必定是有效的.

算法 2. 检测 *route-space* 对象 *rs* 与 *route-space* 对象集 *RS* 的有效性.

输入:待检测对象 *rs* 和对象集 *RS*.

输出:不一致的策略对象对集 *RS-Set*.

1) 把 RS 中的所有元素放到线形表 *list* 中
2) 对于 *list* 中的每一个元素α
3) 若 *rs* 与α不满足有效性规则 1 和规则 2
4) 则把$\langle rs,\alpha\rangle$加入 *RS-Set*
5) 返回结果集 *RS-Set*.

然而,在发生冲突时,我们依然难以判断究竟是哪一个 *route-space* 对象有问题.一种可行的简便方法是根据这些 *route-space* 对象产生的时间来判断.比如,先出现在 E-IRR 数据库中的 *route-space* 对象有效.这就引入了 E-IRR 机制中的抢占式注册方式.

抢占式注册.对某前缀策略而言,只要其满足有效性规则 1 和规则 2,该前缀策略就可以被加入到 E-IRR 数据库中.抢占式注册方式最大的特点就是合法策略一旦被注册,非法策略就不能危害到它.这个原则对防范前缀劫持非常有效,因为在 BGP 路由系统中,前缀劫持往往是对已经合法宣告的网络前缀(或子前缀)进行劫持.可以推断,在现实环境中,这个原则在绝大多数情况下对前缀策略的保护也都是有效的.

此外,在 E-IRR 机制具体实施时,可对抢占式注册方式进一步补充以保证前缀策略的有效性.比如,可以先在大型网络运营商之间应用,然后逐渐扩大范围以至全网.若大型运营商比小型运营商先加入 E-IRR,那么该系统

中前缀策略的有效性从一开始就能得到很好的保证.或者,还可以根据自治系统的实际情况,限制每个自治系统可注册的前缀策略数目.

4 安全能力与性能评估

E-IRR机制的设计目标就是为了保护参与自治系统实际宣告的前缀以防范前缀劫持,因而,E-IRR机制的安全能力不仅与参与自治系统的数量相关,而且还与每个自治系统在BGP系统中实际宣告的前缀数目相关.令参与E-IRR的自治系统集合为*E-IRR*,*E-IRR*⊆*ASN*,每个自治系统$\chi(\chi \in ASN)$实际宣告的前缀数目为函数$N(\chi)$,那么,E-IRR机制可以保护的前缀总数为$\sum_{\chi \in E-IRR} N(\chi)$.在本文中,我们定义E-IRR机制的安全能力为函数G,它是E-IRR机制可以保护的前缀总数与当前所有自治系统实际宣告的前缀总数的比值,即

$$G = \frac{\sum_{\chi \in E-IRR} N(\chi)}{\sum_{\alpha \in ASN} N(\alpha)}.$$

我们使用RouteViews项目(www.routeviews.org)公布的BGP路由表快照对E-IRR机制的安全能力进行评估,具体选取时间点为2007年4月6日8时,因为那天没有报道路由泄漏或劫持事件发生.我们发现少数自治系统宣告了大量的前缀,其中AS701和AS7018分别宣告了4 807和1 503个前缀;而大部分自治系统宣告的前缀数少于3个.然后,我们把自治系统按宣告的前缀数进行排序,并假设自治系统按这个顺序加入E-IRR,最终得到的评估结果如图3所示.从图中可以清晰地看出,随着加入自治系统数目的增多,E-IRR机制的安全能力不断增强;特别地,只要20%的自治系统加入E-IRR,就能够保护BGP系统中80%的前缀.

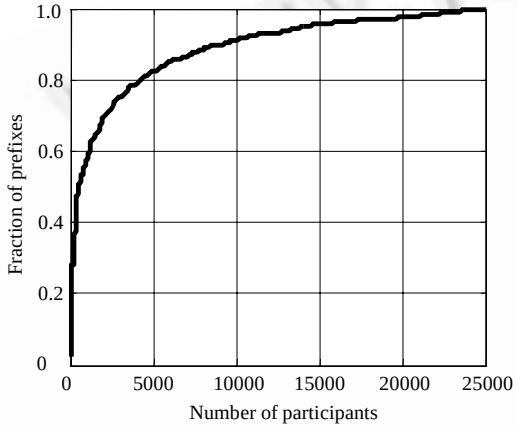


Fig.3 Security capability of E-IRR
图3 E-IRR机制的安全能力

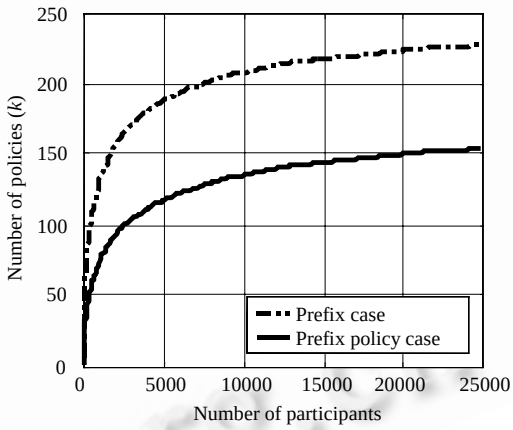


Fig.4 Comparision of policy numbers
图4 策略数目的比较

除了安全能力以外,E-IRR机制在性能方面也有很大的优势.回顾前面对前缀策略的说明,前缀策略关注的是自治系统可宣告的前缀集合,而不是单个的前缀.通常,自治系统拥有的IP地址空间很少变化,但其在BGP系统中宣告的前缀却可能会随着路由策略的变化而变化.当然,如果没有自治系统的帮助,我们难以准确知道每个自治系统真正拥有的IP地址空间,进而无法知道前缀策略的数目.在评估中,我们采用了一个近似的办法来估算前缀策略数量的上界:计算每个自治系统宣告的最大父前缀数,而忽略掉那些子前缀.

利用同一个BGP路由表快照,我们比较了当前所有自治系统的宣告前缀和前缀策略的数目,如图4所示.从图中可以看到,前缀策略的数目随着加入E-IRR的自治系统数目的增加而增大;但是,与实际宣告的前缀数目相比,前缀策略的增长趋势要缓慢得多,总数目大概减少了30%.

5 讨 论

在弱攻击的环境中,我们估计抢占式注册方式能够起到很好的效果.但是,为了使 E-IRR 机制实际有效地运作,我们还需要讨论与抢占式注册方式相关的几个问题.

① 防范非法抢占注册的问题.这个问题可以分两种情况来说明,一种是无意的抢占注册,另一种是恶意的抢占注册.但无论哪种情形,都会导致真正的、有效的策略对象不能注册成功.其实,这未尝不是一件好事:首先,若有效对象加入不了 E-IRR 数据库,这正好帮助验证了系统中已有对象的有效性,暴露出存在的问题.而且,无效的前缀策略会影响相关自治系统的连通性,使得 E-IRR 数据库中的问题更容易被发现.其次,对于无意的抢占注册,可以通过网络运营商之间已有的交涉渠道解决.比如,可求助于 NANOG 网络论坛(www.nanog.org);而对于恶意的抢占注册,则需要成立一个中立组织来维护 E-IRR 数据库,以进行最后的冲突裁决,这样的情况最为麻烦.这主要是考虑到这种情况比较少,而且人工裁决的准确性高,能够解决恶意注册的问题.

② 保护未分配 IP 地址空间的问题.本文的 E-IRR 机制并没有考虑如何保护未分配的 IP 地址空间,因为我们设计 E-IRR 机制的目地是防范前缀劫持,也就是说,保护已分配的 IP 地址空间.然而,如果不能解决这个问题,E-IRR 机制谅是不完整的,有效的方法应该能够保护整个 IP 地址空间.如果未分配的 IP 地址空间随后被分配出去,这个问题转而就变成了第 1 个问题;更为严重的是,对未分配 IP 地址空间的抢占注册很可能是恶意的.为此,我们设想把 5 个 RIR 以及 ICANN 作为特殊的实体引入 E-IRR 机制,让它们首先注册保护未分配的 IP 地址空间.由于这些 IP 地址空间没有与特定的自治系统相对应,所以这些实体定义的对象可能需要重新设计.每当 ICANN 或者各个 RIR 进行了 IP 地址分配,就要更新相应的注册信息,从而使得网络运营商能够注册.采用这种办法,E-IRR 机制就能保护未分配的 IP 地址空间.

③ 反复请求冲突裁决的问题.恶意攻击者可能反复地请求冲突裁决,这会给裁决机构带来麻烦.但这个问题可以通过以下办法来解决:首先,严格控制可在 E-IRR 数据库中注册前缀策略的网络管理员,确保其为相应自治系统的合法网络管理员.这应该不成问题,因为各个 RIR 的 whois 数据库中记录有他们的 E-mail 地址,可以通过这些地址与他们取得联系.其次,记录每个网络管理员申请裁决的历史信息,对于冲突裁决失败过多的网络管理员可以给予一定的惩罚,比如公开该网络管理员的恶意行为或者取消其注册前缀策略的权利.

尽管在 E-IRR 机制中引入了“冲突裁决”,但我们不期望过多地进行冲突裁决.因为这不是我们的本意,E-IRR 机制的有效性体现在它能够帮助多个自治系统管理员协作地、共同地防范前缀劫持.当然,若要求完全的安全保障,那就最好等待互联网资源证书方案的全面实施.

6 结论及工作展望

本文提出的 E-IRR 机制能够帮助网络运营商快速、协作、有效地防范前缀劫持攻击.该机制在前缀劫持的防范能力与安全机制的实际部署需求之间达到了一个较好的平衡,可逐步地实际部署,并且不需要对 BGP 协议进行任何安全扩展.这些特性使得它有望实际可行地解决互联网域间路由系统中的前缀劫持问题.

本方法提出了一种可行的保护互联网 BGP 路由安全的思路,将来的工作主要集中在前缀策略交换机制、网络运营商之间的信任模型以及量化评估抢占式注册方式的有效性等方面.而且,互联网域间路由系统是一个典型的自组织系统,如何借鉴自组织的相关理论来维护 BGP 路由安全可能是一个值得探讨的方向.

致谢 感谢审稿人指出初稿中的错误以及提出的宝贵意见.

References:

[1] Rekhter Y, Li T, Hares S. A border gateway protocol 4 (BGP-4). IETF, RFC 4271, 2006.
[2] Nordström O, Dovrolis C. Beware of BGP attacks. ACM SIGCOMM Computer Communications Review, 2004,34(2):1−8.
[3] Bono VJ. 7007 Explanation and Apology. 1997. http://www.merit.edu/mail.archives/nanog/1997-04/msg00444.html
[4] Popescu AC, Premore BJ, Underwood T. Anatomy of a leak: As9121. 2005. http://www.nanog.org/mtg-0505/underwood.html
[5] Farrar J. C&W routing instability. 2001. http://www.merit.edu/mail.archives/nanog/2001-04/msg00209.html

[6] Atkinson R, Floyd S. IAB concerns & recommendations regarding internet research & evolution. IETF, RFC 3869, 2004.
[7] Kent S, Lynn C, Seo K. Secure border gateway protocol (S-BGP). IEEE Journal on Selected Areas in Communications Special Issue on Network Security, 2000,18(4):582−592.
[8] Xu K, Xiong YQ, Wu JP. Security extension of border gateway protocol BGP-4. Acta Electronica Sinica, 2002,30(2):271−273 (in Chinese with English abstract).
[9] White R. Securing BGP through secure origin BGP. Internet Protocol Journal, 2003,6(3):15−22.
[10] Subramanian L, Roth V, Stoica I, Shenker S, Katz RH. Listen and whisper: Security mechanisms for BGP. In: Robert M, ed. Proc. of the 1st Sym. on Networked Systems Design and Implementation (NSDI 2004). Berkeley: USENIX Association, 2004. 127−140.
[11] Kranakis E, Wan T, Oorschot PC. On interdomain routing security and pretty secure BGP (psBGP). ACM Trans. on Information and System Security (TISSEC), 2007,10(3):1−41.
[12] Karlin J, Forrest S, Rexford J. Pretty good BGP: Improving BGP by cautiously adopting routes. In: David L, ed. Proc. of the IEEE Int'l Conf. on Network Protocols. Washington: IEEE Computer Society Press, 2006. 283−292.
[13] 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 and Distributed System Security Symp. 2003. 75−85. http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/5.pdf
[14] Lad M, Massey D, Pei D, Wu YG, Zhang BC, Zhang LX. PHAS: A prefix hijack alert system. In: Proc. of the 15th USENIX Security Symp. Berkeley: USENIX Association, 2006. 153−166.
[15] Liu X, Zhu PD, Mi Q, Yang MJ. A rules-based approach to anomaly detection in inter-domain routing system. Journal of National University of Defense Technology, 2006,28(3):71−76 (in Chinese with English abstract).
[16] White R. Graph overlays on path vector: A possible next step in BGP. Internet Protocol Journal, 2005,8(2):13−21.
[17] Siganos G, Faloutsos M. Neighborhood watch for Internet routing: Can we improve the robustness of Internet routing today? In: Proc. of the IEEE INFOCOM. Washington: IEEE Computer Society Press, 2007. 1271−1279.
[18] Villamizar C, Alaettinoglu A, Meyer D, Murphy S. Routing policy system security. IETF, RFC 2725, 1999.
[19] Lynn C, Kent S, Seo K. X.509 Extensions for IP addresses and AS identifiers. IETF, RFC 3779, 2004.
[20] Walker D. RIPE database reference manual. RIPE, RIPE-419, 2007.
[21] Zhao XL, Pei D, Wang L, Massey D, Mankin A, Wu SF, Zhang LX. An analysis of BGP multiple origin AS (MOAS) conflicts. In: Christophe D, ed. Proc. of the 1st ACM SIGCOMM Workshop on Internet Measurement (IMW 2001). Washington: ACM Press, 2001. 31−35.
[22] Meyer D, Schmitz J, Orange C, Prior M, Alaettinoglu C. Using RPSL in practice. IETF, RFC 2650, 1999.
[23] Aiello W, Ioannidis J, McDaniel P. Origin authentication in interdomain routing. In: Sushil J, ed. Proc. of the 10th ACM Conf. on Computer and communications security (CCS 2003). Washington: ACM Press, 2003. 165−178.

附中文参考文献:

[8] 徐恪,熊勇强,吴建平.边界网关协议 BGP-4 的安全扩展.电子学报,2002,30(2):271−273.
[15] 刘欣,朱培栋.基于规则的域间路由系统异常检测.国防科学技术大学学报,2006,28(3):71−76.

刘欣(1978－),男,湖南常德人,硕士,主要研究领域为互联网域间路由.

彭宇行(1967－),男,博士,教授,博士生导师,主要研究领域为并行与分布处理技术,计算机网络技术.

朱培栋(1971—),男,博士,副教授,CCF 会员,主要研究领域为路由技术,移动网络,网络安全.