ISSN 1000-9825, CODEN RUXUEW
Journal of Software, Vol.21, No.7, July 2010, pp.1704−1716
doi: 10.3724/SP.J.1001.2010.03573

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

域间 IP 欺骗防御服务增强机制*

吕高锋+, 孙志刚, 卢锡城

(国防科学技术大学 计算机学院,湖南 长沙 410073)

Enhancing the Ability of Inter-Domain IP Spoofing Prevention

LÜ Gao-Feng+, SUN Zhi-Gang, LU Xi-Cheng

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

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

Lü GF, Sun ZG, Lu XC. Enhancing the ability of inter-domain IP spoofing prevention. *Journal of Software*, 2010,21(7):1704−1716. http://www.jos.org.cn/1000-9825/3573.htm

Abstract: The validation of source IP addresses becomes the key technique for devising a trustworthy network. However, inter-domain IP spoofing preventions based on source-destination labels and end-hosts IP authentications based on source labels both adopt end to end mode to solve the problem, which ignores the flooding of spoofing packets on middle networks. To address this problem, an enhancing mechanism for the inter-domain IP spoofing prevention service, ESP (enhanced spoofing prevention), is proposed. Via integrating path labels into source labels, ESP reduces the collision of source labels at destination networks and enables filtering IP spoofing packets toward other nodes in middle networks, thus prevents flooding attacks in advance and extends the protected domain of the spoofing prevention. Based on BGP (border gateway protocol) update ESP develops the validation of prefix security to restrict the scope of the propagation of labels, thus decreases the cost of computing and storing of labels. The abilities of IP spoofing prevention and filtering spoofing packets in advance are demonstrated in the topology, which is constructed based on RIB (routing information base) provided by Routeview.

Key words: IP spoofing prevention; BGP (border gateway protocol); trustworthy network

摘 要: IP 地址真实性验证成为构建可信网络的基础,基于源-目的标识(密钥)的自治域级 IP 欺骗过滤和基于源标识(公钥)的端系统级 IP 认证均采用了端-端方式试图解决 IP 欺骗.端-端认证方式实现简单,但却忽略了 IP 欺骗报文对中间网络的泛洪攻击,防御效果差.提出面向 IP 欺骗防御联盟成员的域间 IP 欺骗防御服务增强机制——ESP(enhanced spoofing prevention).ESP 引入开放的路由器协同机制,提供了源-目的路径中 ESP 节点信息通告和协同标记的框架.基于源标识 IP 欺骗防御,ESP 融入了路径标识,不仅减小了源标识冲突概率,而且混合型标识支持了 ESP 节点根据报文标识提前过滤 IP 欺骗报文.基于 BGP(border gateway protocol),提出前缀 *p*-安全节点的概念和检测理论,有效控制了源标识传播范围,减小了 ESP 节点的标记和过滤开销.ESP 继承了基于标识的防御机制的可部分部署性,能够很好地支持动态路由和非对称路由.应用 Routeview 提供的 RIB(routing information base)进行评估,ESP 增强了 IP 欺骗防御服务的能力,而且能够提前过滤 IP 欺骗报文.

* Supported by the National Basic Research Program of China under Grant Nos.2005CB321801, 2009CB320503 (国家重点基础研究发展计划(973))

Received 2008-07-28; Accepted 2008-12-29

关键词: IP 欺骗防御;BGP(border gateway protocol);可信网络
中图法分类号: TP393 文献标识码: A

目前,Internet 默认主机将自己的 IP 地址写入报文源 IP 地址域,然而缺乏安全机制验证该假设[1].攻击者将伪造的 IP 地址写入报文源 IP 地址域,扮演其他人或隐藏报文的起源,产生源 IP 地址欺骗.源 IP 地址欺骗以多种方法破坏了 Internet 的安全性和可用性:

- 首先,它支持反射攻击.攻击者发送请求,将报文源地址伪造为受害者 IP 地址,欺骗目的端主机向受害者应答并发送数据;
- 其次,IP 欺骗使得防御机制复杂化.因为 IP 欺骗报文攻击流表现为来源于多个位置,防御机制不能使用报文源 IP 地址过滤攻击流,因为这样会对合法主机(如被伪造的主机)的数据流造成危害;
- 再次,IP 欺骗使干扰双方通信成为可能.在加密的安全通道下通过注入报文,导致 TCP 连接劫持,DNS (domain name system) cache 失效;
- 最后,IP 欺骗破坏了流量控制机制的假设,使用公平队列在不同流之间分配资源.

IP 欺骗防御机制是对网络安全研究的重大挑战.虽然有些大规模 Internet 攻击不使用 IP 欺骗的方法,如分布式拒绝服务攻击(distributed denial of service,简称 DDoS)以及各种网络蠕虫,因为这些攻击不需要欺骗,大量分布式攻击代理足够使受害者服务瘫痪[2],然而忽视 IP 欺骗机制的威胁也是短视的,因为随着 DDoS 攻击和蠕虫防御机制开始部署,IP 欺骗又将成为具有吸引力的绕开已部署的防御机制的方式[3].

已有的 IP 欺骗防御机制存在诸多不足:基于路由的 IP 欺骗报文过滤机制[4]根据节点的路由信息过滤每个端口不期望的报文,能够提前过滤 IP 欺骗报文,但是此类机制不能很好地适应网络拓扑的动态变化,存在误操作;基于源-目的标识(密钥)的自治域级 IP 欺骗过滤[5]和基于源标识(公钥)的端系统级 IP 认证[6]均采用了端-端方式解决 IP 欺骗.端-端方式实现简单,但却忽略了 IP 欺骗报文在网络中转发过程中所造成的带宽消耗等危害,而且防御效果较差.

设计高效的、易于部署的 IP 欺骗防御机制成为当务之急.针对提前过滤 IP 欺骗报文和防止带宽攻击的目标,本文提出了一种面向 IP 欺骗防御联盟成员的域间 IP 欺骗防御服务增强机制 ESP(enhanced spoofing prevention),防御节点不仅验证发送给自己的报文,而且验证转发给其他节点的报文.为了支持源-目的路径中 ESP 节点信息通告和协同标记与验证,引入开放的路由器协同机制,增强了防御节点过滤能力.为了减小源标识冲突概率,ESP 在源标识中融入路径标识,而混合型标识支持了 ESP 节点根据报文标识提前过滤 IP 欺骗报文.为了控制源标识的传播范围,提出前缀 p-安全节点的概念和检测理论,减小了 ESP 节点的标记和过滤工作量.ESP 增强了 IP 欺骗防御节点的能力,而且能够提前过滤 IP 欺骗报文.ESP 继承了基于标识的防御机制的部分部署性,具有较高的部署激励.

本文第 1 节概述相关研究工作.第 2 节介绍域间路由系统,重点阐述 ESP 设计思想.第 3 节详细描述 ESP 设计与实现,分析算法复杂度和正确性.第 4 节通过实验模拟说明 ESP 的过滤能力,并与已有防御机制进行比较.第 5 节总结全文并指出下一步的研究方向.

1 相关研究

Ingress 过滤[7]机制能够在报文离开本地网络之前过滤具有非法源地址的 IP 欺骗报文,然而 Ingress 过滤的有效性依赖于大范围部署,而且向早期的部署者提供了很少的激励.即使 ISP 部署了 Ingress 过滤,也没有向 ISP(Internet service provider)的客户提供欺骗防御相关的利益,只是向其他 ISP 的客户提供了 IP 欺骗报文过滤服务.

反向路径转发 RPF(reverse path forwarding)[8]是 Ingress 过滤的扩展,使用 IP 路由表过滤 IP 欺骗报文.RPF 成为一个可选的主流路由器功能,只转发具有合法源 IP 地址的报文,能够减轻 IP 欺骗造成的危害.如果报文的入口与用报文源 IP 地址查找路由表获得的结果一致,那么该报文具有合法的源 IP 地址.然而,RPF 受拓扑限制,

只能用于对称路由环境中.类似于 Ingress 过滤,RPF 不能向部署者提供欺骗报文过滤相关的利益.

基于路由的分布式报文过滤机制 DPF(distributed packet filter)[4]使用路由信息过滤 IP 欺骗报文,DPF 部署者根据从源到目的的转发路径是否经过自己来判断 IP 欺骗报文,如果不经过,则该报文为 IP 欺骗报文.DPF 过滤器可以部署在枢纽型 AS(autonomous system)中,因此只需要部分网络部署,就可以显著过滤大部分 IP 欺骗报文.但是 DPF 也不能向部署者提供直接的激励,所有的部署者共享 IP 欺骗防御服务获得的利益.

Ingress 过滤、RPF 和 DPF 机制可以归结为基于路由的源端过滤,在距离攻击者最近的过滤器中过滤 IP 欺骗报文.其优点是能够提前过滤 IP 欺骗报文,而且没有通信开销,计算开销也很小;它们共同的不足是对动态路由的适应能力、自我保护能力以及部署激励都较差.

SPM(spoofing prevention method)[9]首次提出基于标识的域间 IP 欺骗防御机制.通过专有协议在源 AS 与目的 AS 之间共享与源-目的 AS 对关联的标识和源 IP 地址空间,并将标识通告给域内所有边界路由器,同时,周期性地更新该标识.源端 AS 边界路由器使用源-目的标识标记发出报文,而目的端 AS 通过验证入报文标记的正确性,识别 IP 欺骗的报文.SPM 可以识别伪造 SPM 成员 IP 地址的欺骗报文.

Pi(path identification)[10]是一种基于路径标识的被动过滤机制.源于相同节点的报文具有相同的路径标识,受害者识别攻击报文标识后,即可用于过滤后续攻击报文,保护自己的网络.Pi 标识是基于报文 TTL(time to live),将 TTL 作为 IP 的 ID 域索引,路由器将自己的标识插入该位置.传统路由器对该机制有负面影响,因为它们减小了 TTL 值,但是没有插入标记,形成标记黑洞.

StackPi[11]机制采用基于栈的插入标识方式克服了该问题.把 ID 域作为栈,路由器将标识压入栈,则标识是相邻的.StackPi 节省了记录空间,能够记录更多的路由器标识.在完全部署的情况下,Pi 和 StackPi 是相同的.

SPM,Pi,StackPi,PPM(probabilistic packet marking)[12]机制是典型的基于标识的目的端过滤 IP 欺骗报文的机制.与源端过滤机制相反,它们能够直接向部署者提供激励.然而其代价是记录标识的存储开销,以及标记和验证报文的处理开销.

BASE(BGP anti-spoofing extension)[13]是一种动态的防欺骗机制,分为标记发布阶段、触发阶段、报文标记和过滤阶段以及撤销阶段. BASE 采用了链式标识,不主动更新标记,只有在路径发生改变时才更新标记传播路径.链式标记增加了攻击者破解标记的难度.然而,路由器标识的计算和发布方式确定了 BASE 不用重新计算标识,只是根据新的路由重新发布标识,标识的确定性减弱了标识安全度.另外,BASE 链式标识在每跳重写标识,不仅开销大,还不利于追踪报文源.若要查找攻击源,必须迭代回溯.当目的端系统检测到受恶意报文攻击时,才向源端系统发送报文标记请求.这种被动防御机制存在着检测恶意报文攻击和源端响应请求标记报文的延迟.

本文提出的面向 IP 欺骗防御联盟成员的域间 IP 欺骗防御服务增强机制 ESP,融合了源标识和路径标识.与 BASE 比较,ESP 标识的计算和存储开小,而且不受路由更新约束.新的标识机制支持了中间网络过滤(包括源端过滤)和目的端过滤相结合的混合型防御机制,增强了防御节点的能力,而且能够提前过滤 IP 欺骗报文.

2 域间 IP 欺骗防御

2.1 域间路由

用图 $G=(V,E)$表示 Internet,节点 $v\in V$ 表示自治域 AS,边 $e(u,v)\in E$ 表示相邻 AS u,v 之间的 BGP 会话.假设相邻 AS 之间最多有一条边,每个节点拥有一个或多个网络前缀,节点通过交换 BGP 路由更新消息,路由通告或路由撤销,学习到达目的网络前缀的可达信息[14].路由通告包含路由的属性列表,如路由 r 传播的 AS 序列 *as_path*,用 *r.as_path* 表示;目的网络的前缀 d,用 *r.prefix* 表示,即 $r.as\_path=\langle v_k v_{k-1}\ldots v_1 v_0\rangle$,$r.prefix=d$.同时可知,路由 r 源于节点 v_0,表示为 $r.origin=v_0$,该节点拥有 *r.prefix* 表示的 IP 地址空间.在路由到达节点 v_k 之前,依次经过了节点 $v_1,v_2,\ldots,v_{k-1}$.

由于 AS 内部 BGP 路由器全互连,保证了 BGP 路由器构造的 Internet 拓扑结构是一致的.因此,本文用 AS 路由处理过程代表 AS 内部每个路由器的路由处理过程.BGP 是基于策略的路由协议,最佳路由选择和传播都是由本地定义的路由策略来指导,节点使用了两组路由策略,输入(import)策略和输出(export)策略.如图 1 所示,

其中,邻居相关的输入策略应用到了从邻居学到的路由,邻居相关的输出策略应用到本地选择最佳路由.

节点 u 从 v 收到路由 r,记为 $import_u(v,r)$,表示 u 接受该路由且被输入策略修改.u 接受的路由存储在路由信息表(routing information base,简称 RIB)中,记为 $candidateR_u(d).candidateR_u(d)=\{r|import_u(v,r),r.prefix=d,\forall v\in N(u)\}$,其中,$N(u)$表示节点 u 的邻居.节点 u 从候选路由 $candidateR_u(d)$中选择一条到达目的 d 的最佳路由,记为 $bestR_u(d)$.Export 策略决定了是否应把最佳路由转发给它的邻居,并根据路由策略修改路由属性,节点 u 在应用邻居相关的 export 策略之后向它的邻居 w 输出最佳路由 $r=bestR_u(d)$,记为 $export_u(w,r)$.

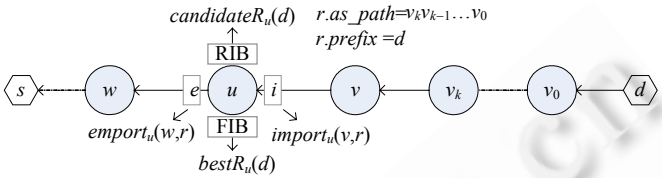


Fig.1 BGP decision

图 1 BGP 路由决策

2.2 基本原理

定义 1(IP 欺骗报文). 报文源 IP 不是报文发送者的 IP 地址.

定义 2(上游邻居). 当报文 m 在源点 s 到目的节点 t 路径中转发,到达节点 v,在 v 到源点 s 的候选路径中,v 的邻居的集合记为 $upstreamN_v(s)$,则

$$upstreamN_v(s)=\{w|export_w(v,r),r=bestR_w(s)\} \tag{1}$$

显然,在 Internet 中,当报文从源点转发到目的节点时,路径中各节点的 $upstreamN_v(s)$在不断地增加.这是 Internet 连通性的表现,距离源点越远的节点,可以选择更多的邻居到达源节点.另一方面,随着距源点的跳步数的增加,$upstreamN_v(s)$随之增长,报文源点的位置在逐渐隐藏,即离源点越远,越难回溯到报文源,这是 Internet 不可逆的表现.$upstreamN_v(s)$的增长扩大了防御节点观察到的源点所属的 IP 地址空间,加剧了判断报文源 IP 地址所属关系的复杂度,从而增加了过滤源 IP 欺骗报文的难度.

为了防止源 IP 地址欺骗,最直观的方法是记录转发报文过程中上游邻居信息,如,可以在报文中加入邻居信息,变不可逆转发路径为可逆,增强网络可控性.已有的防御机制,如基于 BGP 路由的 IDPF(inter-domain packet filter)[15],由于路由只与节点的接口关联,不能区分转发路径中的上游节点,仍然出现了上游邻居增长的问题.因此,基于路由的防御机制不能识别从源到目的节点路径中节点伪造源节点 IP 的欺骗报文.而基于源-目的标识的 SPM 克服了该局限性,报文标识指示了报文源.因此,本文选择以基于标识的 IP 欺骗防御机制为基础设计域间 IP 欺骗防御机制.

然而,在基于标识的域间 IP 欺骗防御机制中,源端 c 和目的端 d 自治域共享源端有效 IP 地址空间和源-目的对标识 k_c^d,源端 c 的边界路由器标记发出报文,目的端 d 的边界路由器根据标识验证入报文源地址的合法性,即只能在目的端检测报文是否伪造 IP 地址,如图 2(a)所示.如果攻击者针对阻塞目的端 d 的网络连接 b-d,发送大量的恶意报文消耗目的端 d 的网络连接 b-d 的带宽,尽管目的端 d 能够过滤 IP 欺骗报文,但是 DDoS 攻击已经对其连接 Internet 的链路 b-d 造成堵塞,从而影响了合法用户的访问.为了满足提前过滤的设计目标,如果防御机制在离攻击源最近的防御节点 b 中过滤 IP 欺骗报文,那么就可以提前阻止针对目的端网络的带宽攻击,而且可以最大限度地减小攻击流的危害.因此,在基于标识的 IP 欺骗防御的基础上,本文进一步提出了增强域间 IP 欺骗防御服务的机制 ESP,在源端到目的端的路径中防御节点 b 中共享源-目的端标识 k_c^d 和有效源 IP 地址空间,从而支持 b 提前过滤伪造源端网络地址攻击目的端网络 d 的 IP 欺骗报文,如图 2(b)所示.

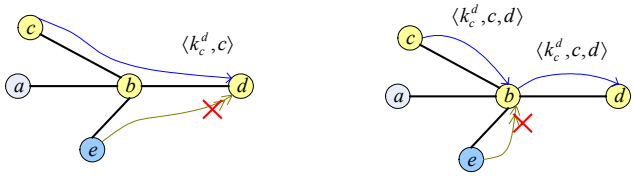


Fig.2 Filtering at destination and middle networks

图 2 目的端和中间防御节点过滤比较

2.3 关键技术

定义 3(ESP 节点). 支持 IP 欺骗防御服务增强机制的防御节点,称为增强型 IP 欺骗防御节点,简称 ESP 节点.

定义 4(ESP 网络). 网络中,所有 ESP 节点基于专用交互协议连接起来构成的虚拟叠加网络,称为 ESP 网络.

定义 5(ESP 标识). ESP 节点插入报文的与源点和转发路径相关的信息.

定义 6(源 IP 地址空间). 源点有效 IP 地址的集合,通常表示为网络前缀.

2.3.1 标识方式

标识可以分为源标识和源-目的对标识.首先分析采用不同标识方式,由于共享标识防御节点需要额外的计算资源和存储资源,若采用源-目的对标识,在 ESP 中各防御节点代理任意源-目的对标识,记录源-目的端标识,可以完全过滤 IP 欺骗报文.然而,源-目的对标识的数目是 $2\times n^2$(源-目的对标识有方向性),其中,n 为 ESP 节点数目.节点的计算和存储开销将会是巨大的,可行性较差;若采用源标识方式,标识数目减小为 n,那么 ESP 节点需要记录的标识只有 n 个,极大地减小了节点计算、存储和通信开销.在 ESP 节点共享任意防御节点标识机制下的情况,这是一种可行的标识方式.

ESP 节点 s 生成源标识 oid_s,并向其他 ESP 节点通告 oid_s 与网络前缀 $pref_s$(有效源 IP 地址空间),记为 $pref_s$=$Source(oid_s)$.当 ESP 节点 v 接收到报文 m 时,根据报文 m 中包含的 oid_s 即可推导出报文源节点 s 的 IP 空间 $pref_s$.可以看出,在报文中插入源标识增加了报文源信息,而且该信息在报文转发过程中保持不变,那么下游节点就可以回溯真实的报文源,将不可逆的网络转化为可逆的网络,而且增强了网络的可控性.

2.3.2 冲突消解方式

定义 7(标识冲突). 若防御节点接收到两个源的标识相同,则无法区分该标识对应的源空间,发生标识冲突.

如果节点 e 从 ESP 节点 a 和 c 接收到相同的源标识,即 $h_c(c)=h_a(a)=oid_0$,那么 $Source_e(oid_0)$是一对多映射,即 oid_0 对应于多个源 a 和 c.对应于多个源 IP 地址空间,则节点 e 无法根据报文的源标识判定报文的源 IP 地址是否与源点 IP 地址空间相一致,如图 3(a)所示.ESP 节点在报文中插入源标识后,标识冲突又影响了节点回溯报文源,其间,节点 c 可能冒充节点 a 的源 IP 地址,即仍然存在 IP 欺骗的可能.

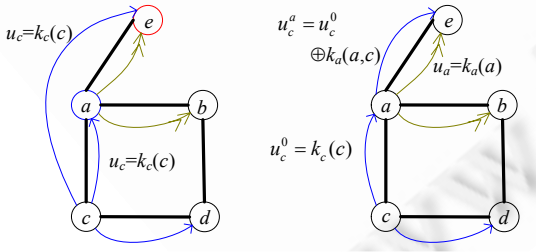


Fig.3 Collision and resolution of labels

图 3 标识冲突和消解

冲突是源标识饱和引起的报文源不确定性增加,可以继续向报文中插入路径信息,增强报文源可回溯性和可控性.BASE 路由器采用了替换原有标识以防止标识冲突.ESP 采取增加路径标识的方法,在报文中插入部分路径标识 pid,增加报文源的回溯性,使 ESP 节点能够检测 IP 欺骗报文,如图 3(b)所示.这样,ESP 标识由开始的源标识 oid 融入路径标识 pid,不断增加报文位置信息以解决标识冲突,增强 ESP 节点分辨 IP 欺骗报文的能力.

3 ESP 设计

3.1 ESP标识

3.1.1 标识计算

假设 ESP 节点有密钥 *key*,利用它来计算 ESP 源标识.AS 边界路由器对每个出报文进行标记,同时过滤不具有正确标记的入报文.ESP 标识是在源标识中融入路径标识而形成的,即 $esp=\{oid,pid\}$.ESP 节点 s 首先生成源标识 oid_s 作为 ESP 标识 $esp_0 \rightarrow oid$ 的初始值,并通告给其他 ESP 节点.其他 ESP 节点在转发 ESP 标识时,用路径信息更新该标识,即在源标识中加入路径标识 *pid*.设 ESP 标识传递路径为 $path(s,t)$,即 $path(s,t)$表示从源节点 s 到目的节点 t 的路径中 ESP 节点的有序集合,$path(s,t)=\{v_1,v_2,\ldots,v_n\}$,其中,$v_1=s,v_n=t$.节点 v_i 收到 v_{i-1} 通告的原点 s 的 ESP 标识及源 IP 地址空间,记为 $v_{i-1} \mapsto v_i:\{esp_s,p_0\}$,并更新该标识,则

$$esp_i \rightarrow pid=((esp_{i-1} \rightarrow pid)<<n) \oplus hash(k_i,v_{i-1},v_i) \tag{2}$$

其中,$esp_0 \rightarrow oid=h(k_0,v_0)$,$esp_0 \rightarrow pid=0$,$k_i$ 是节点 v_i 的密钥,v_i 是表示该节点的 IP 地址.ESP 节点 a 的 ESP 标识计算以及传递过程如图 4 所示.Hash 函数可以采用伪随机函数 PRF(pseudo-random function)[16],PRF 有两个参数:密钥和输入,产生输出.只要密钥是保密的,输出近似为随机数.根据 ESP 标识计算和传递过程可知,ESP 标识融合了源标识 *oid* 和路径标识 *pid*,而且路径标识 *pid* 是标识链,能够减小标识被伪造的可能性.路径标识可以提前计算,当 ESP 节点触发更新之后,一起更新路径标识.

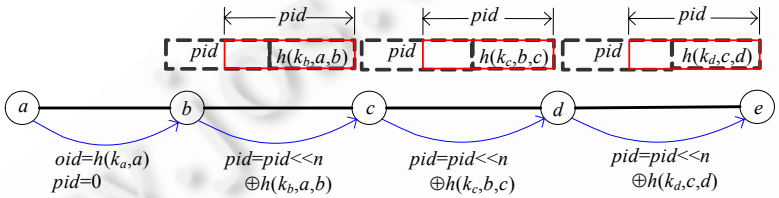


Fig.4 Propagation and computing of ESP

图 4 ESP 标识传递与计算

在 ESP 机制的实现过程中,源标识子域 *oid* 和路径标识子域 *pid* 分别为 16 比特.源标识域和路径标识域由源节点初始化.在报文转发路径中,ESP 节点按照基于栈的路径标记方法插入该节点的路径标识.有两种方式:一种是路径标记有全局统一的参数 n,每个节点插入报文的路径标识大小相同;另一种方式是 ESP 节点自己选择特定大小 n 标记,可以获得空间效率.如路由器只有两个接口,标识为 2 比特,尽管该路由器不影响路径,但因为它可以被抽象为一条链路,所以每个路由器根据自己的接口数计算路径标识的大小 n.

3.1.2 标识传递

ESP 节点之间共享信息可以采用多种方法:一种方法是通过 BGP 更新消息在路由器之间传递信息;另一种是设计发布协议,如 SPM 等.若使用 BGP 协议,则防御机制很容易发布标识以及维护最新的标识信息,然而根据 AS 路由策略,在非对称环境中使用 BGP 消息存在错误肯定的问题;另外,基于 BGP 更新消息共享过滤信息,存在传统 BGP 路由器的 AS 路由策略阻止 update 消息传播到邻居,造成基于 BGP 传递消息的通信机制的失效问题.ESP 设计了开放的路由器协同协议更新标识和有效源地址空间,避免了因传统 BGP 路由器的 AS 路由策略阻止 update 消息传播到邻居造成的基于 BGP 传递消息的通信机制的失效.

定义 8(p-源节点). 网络前缀 p 的拥有者.在正常情况下,源 IP 地址属于 p 的报文的发送者.

定义 9(p-安检节点). 对源 IP 属于前缀 p 的报文进行基于标识的 IP 欺骗报文过滤的节点.

定义 10(p-安全节点). 接收到的源 IP 属于前缀 p 的报文是非 IP 欺骗报文,不需要进行基于标识的 IP 欺骗报文过滤的节点.

引理 1. 通过 p-安检节点的源 IP 属于前缀 p 的报文是非 IP 欺骗报文.

证明:根据 p-安检节点的定义可知,p-安检节点需要对接收的源 IP 属于前缀 p 的报文进行基于标识的 IP 欺

骗过滤.如果报文没有伪造属于前缀 p 的 IP 地址,则 p-安检节点会向下游节点转发该报文;否则,过滤.显然,通过 p-安检节点的源 IP 属于前缀 p 的报文是非 IP 欺骗报文. □

定理 1. 若上游邻居是 p-安全节点或 p-安检节点,则该节点也是 p-安全节点.

证明:首先,将节点的邻居分为上游邻居和非上游邻居.

- 如果 ESP 节点 v 的非上游邻居节点 w 向它转发源 IP 属于 p 的报文,那么节点 v 根据 $u\notin upstreamN_v(s)$ 可以判定报文是 IP 欺骗的;
- 如果 ESP 节点 v 的上游邻居节点 $w(w\in upstreamN_v(s))$是 p-安检节点,根据引理 1 可知,上游 p-安检节点转发的是非 IP 欺骗报文,节点 v 无需再次检查;
- 如果 ESP 节点 v 的上游邻居节点 $w(w\in upstreamN_v(s))$是 p-安全节点,根据定义 3 可知,上游节点接收到的报文是非 IP 欺骗报文,而且自己也不会产生 IP 欺骗报文,节点 v 无需再次检查.

综上所述,接收到的源 IP 属于前缀 p 的报文是非 IP 欺骗报文,不需要进行基于标识的 IP 欺骗过滤的节点.即该节点是 p-安全节点. □

从定理 1 可知,p-安全节点具有传递性.当且仅当上游邻居节点都是 p-安全节点,p-安全性才可以向下游传递.根据上游邻居的定义,由于 Internet 路由的非对称性,上游邻居只是到达源 s 的可行路径,并不是源 s 到达该节点的可行路径,因此存在上游邻居不是 p-安全节点,阻碍了 p-安全性的传递.这也是需要在转发路径上 ESP 节点中对其他节点发送的报文进行检查的原因.

ESP 标识传递如算法 *espPropagation* 所示:ESP 节点主动向其他 ESP 节点通告 ESP 标识和网络前缀(有效源 IP 地址空间),当节点 v 接收到节点 u 通告的标识和网络前缀(有效源 IP 地址空间),即 $u\mapsto v:\{esp_u,p_0\}$时,首先判断信息是否正确,也就是节点 u 是否为节点 v 的上游邻居节点,如算法的第 1 步所示;其次,检查是否已建立关于该网络前缀的标识,如算法的第 2 步描述;如果已经建立,则不需要重新建立.否则,更新标识,即向标识中加入路径信息,如算法的第 3 步描述;最后,向下游邻居节点通告更新后标识和网络前缀.根据标识计算方式可知,只需向 RIB 中到达目的地的路由中第 1 个 ESP 节点通告,如算法的第 4 步~第 8 步所描述的那样;同时,节点 v 检查是否所有的上游邻居均通告了关于该网络前缀的标识,如算法的第 9 步~第 12 步所描述的那样.如果是,则节点 v 成为该网络前缀的安全节点;否则,不是.

算法 1. *espPropagation*(esp_u,p_0).

1. if $(u\mapsto v:\{esp_u,p_0\})$ & $(u\in upstreamN_v(p_0))$
2. if $(p_0\notin Filter_v)$ {
3. $(esp_v\rightarrow pid)\leftarrow((esp_u\rightarrow pid)<<n)\oplus h(k_v,u,v)$;
4. for each $pref_i\in RIB_v$ {
5. $r\leftarrow bestR_u(pref_i)$;
6. $w\leftarrow selectESP(r)$;
7. if $(w\notin upstreamN_v(p_0))$
8. $v\mapsto w:\{esp_v,p_0\};\}\}$
9. for each $u_i\in upstreamN_v(p_0)$
10. if $(u_i\mapsto v:\{esp_{u_i},p_0\})$
11. $p\text{-}sec_i\leftarrow 1$;
12. $p\text{-}sec_v\leftarrow$ & $p\text{-}sec_i$;

根据算法执行过程可以看出,ESP 节点只需要遍历 RIB 表,向下游 ESP 节点通告源 IP 地址空间和更新后 ESP 标识,算法复杂度为 $O(n)$.

3.1.3 标识域

ESP 在部署过程中重载了已有的报文域,IP 报头中 16 比特的 ID 域.目前,该域用来区分属于不同报文的 IP 分片.ESP 节点用 ID 域记录源标识.当 ID 域被用来记录源标记时继续保留 Flag 域和 Offset 域也没有任何意义,

因此,ESP 节点又应用 3 比特 Flag 和 13 比特 Offset 域记录路径标识.

3.1.4 标识更新

攻击者可能伪造源标识,冒充 ESP 节点发送的报文,企图获得 ESP 节点发送的正常报文享受的服务质量.攻击者可以通过穷举方式猜测 ESP 标识,因此标识需要周期性更新.ESP 标识由源标识和路径标识组成,首先由 ESP 源点启动标识更新过程,相邻的 ESP 节点收到新的标识后,更新 ESP 标识,并向其他相邻的 ESP 节点通告.

3.2 ESP节点标记

ESP 标识由源标识和路径标识两部分组成,而且只有 ESP 节点才可以生成源标识,非 ESP 节点无法生成源标识.当 ESP 节点 v_i 发送源于自己的报文 m 时,用自己的源标识标记报文,路径标识清零.当 ESP 节点接收到其他节点 v_{i-1} 转发的报文时,将与报文进入的路径信息关联的路径标识压入报文 ESP 标识的路径标识子域.从算法 *espMarking* 的描述可以看出,ESP 节点只需要执行插入标识的操作,源标识或路径标识处理简单,开销非常小.

算法 2. *espMarking*(m).

1. if ($(m \to s) \in pref_{v_i}$) {
2. $oid_i \leftarrow hash(k_i, v_i)$;
3. $pid_i \leftarrow 0$;}
4. else {
5. $oid_i \leftarrow oid_{i-1}$
6. $pid_i \leftarrow (pid_{i-1} << n) \oplus hash(k_i, v_{i-1}, v_i)$;}
7. $mark(m, esp_v)$;

由于重载了 ID 域,则 ESP 节点可以不标记分片报文.网络中分片报文很少,因此对过滤 IP 欺骗报文的效果很小.若攻击者采用分片方式制造恶意数据流,那么未标记的报文也是最先被过滤掉的.

3.3 ESP节点过滤

3.3.1 基于 *esp* 的过滤

ESP 节点 v_i 接收到节点 v_{i-1} 通告的 ESP 标识和有效源 IP 地址空间,即 $v_{i-1} \mapsto v_i : \{esp_{v_{i-1}}, p_0\}$,ESP 节点 v_i 记录源 IP 地址空间与 ESP 标识的映射关系,即 $source_{v_i}(esp_{v_{i-1}}) \to p_0$,并生成过滤表 F_i.当 ESP 节点接收到报文 $m(s,t,esp_0)$时,根据报文源 IP 地址与 ESP 标识索引的有效源 IP 地址空间的关系进行过滤.

对于源于 ESP 节点的报文,ESP 节点用 ESP 标识标记了该报文,在转发路径中的 ESP 节点过滤没有正确标识的入报文.ESP 节点根据报文中 ESP 标识索引的源 IP 地址空间与报文源 IP 地址的所属关系,判断该报文是否为 IP 欺骗报文,如算法 *espFiltering* 的第 1 步~第 4 步所示.ESP 节点为 AS 边界路由器,能够很容易地实现基于路由的报文过滤机制,从而确保源于自己的报文是正确的(或伪造自己内部 IP 的欺骗报文).

算法 3. *espFiltering*(m).

1. if (($m \to esp \to oid$)≠0) {
2. $p_0 \leftarrow source_{v_i}(esp_{v_{i-1}})$;
3. if ($m \to s \notin p_0$)
4. *discard*(m);}
5. else {
6. $ip_0 \leftarrow source_{v_i}(esp_{v_{i-1}} \to pid)$;
7. if ($m \to s \neq ip_0$);
8. *discard*(m);}

3.3.2 基于 *pid* 的过滤

对于源于非 ESP 节点的报文,ESP 标识只有路径标识子域,而且报文源点不会通告有效源 IP 地址空间,因此,转发路径中 ESP 节点不能根据标识索引的源 IP 地址空间判断报文源 IP 地址的正确性.此时,ESP 节点路径标识

pid 过滤 IP 欺骗报文.Internet 报文转发路径相对较稳定,来源于某个网络到达目的地的报文通过了一致的 ESP 节点序列,则这些报文具有比较稳定的路径标识 *pid*;相反地,假设 *pid* 均匀分布,则给定的 *pid* 只能由相对较少的源网络生成[9].这样,报文转发路径中的 ESP 节点则根据稳定的 *pid* 过滤 IP 欺骗报文.

在正常情况下,ESP 节点学习给定网络发出的到达目的网络的报文包含的源 IP 地址和路径标识 *pid*,记为⟨*pid*,IP⟩,即 $source_{v_i}(pid)\rightarrow \text{IP}$,生成过滤表 F_i.当 ESP 节点检测到受到攻击,则使用⟨*pid*,IP⟩过滤源 IP 地址欺骗的报文.对于每个到达的报文,ESP 节点检查报文的⟨*pid*,IP⟩是否与过滤表中记录相匹配,如果报文的二元组不匹配过滤表中对应数据项,则过滤该报文,如算法 *espFiltering* 的第 5 步~第 8 步所示.

与已有的 IP 欺骗防御机制一样,在检查报文是否为 IP 欺骗报文时,需要一次额外查表,查找报文的 ESP 标识或路径标识,获得有效源 IP 地址空间或源 IP,从而判断报文源 IP 地址的所属关系.算法复杂度为 $O(n)$.

3.4 正确性分析

部分部署、动态路由和非对称路由等特殊网络环境对 IP 欺骗防御机制的设计提出了巨大挑战,如果不能很好地解决这些问题,那么 IP 欺骗防御机制部署是不可行的.我们通过分析 ESP 机制在这些环境中的运作,来证明 ESP 机制的正确性.

3.4.1 部分部署

ESP 机制支持部分部署,增强了部署激励,部署者都可以从 ESP 网络获得额外回报.首先说明 ESP 机制在部分部署环境中如何工作.假设在 n 个节点中部署 k 个过滤器,$w_1,w_2,\ldots,w_k\in p(s,t)$,在路径中任何过滤器 $w_i\in p(s,t)$,可以与邻居过滤器 w_{i+1} 建立连接.

图 5 表示了 ESP 在部分部署情况下的运作.通过开放的路由器协同协议,ESP 节点可以和其他非相邻的 ESP 节点通信.网络中,ESP 节点 *a*,*b*,*c* 构成 ESP 虚拟网络,每个 ESP 节点可以标记和过滤欺骗报文.攻击者通过 ESP 节点 *c* 向正常流中注入了 IP 欺骗报文,这些报文将会在 ESP 节点 *c* 处被识别并过滤.即使攻击者通过非 ESP 节点 *d* 向正常流中注入了 IP 欺骗报文,这些报文也将会在下一个 ESP 节点 *e* 处被识别.ESP 节点构成的网络会过滤伪造 ESP 成员地址的 IP 欺骗报文以及非 ESP 节点发送恶意的报文,为 ESP 成员提供了良好的安全服务.

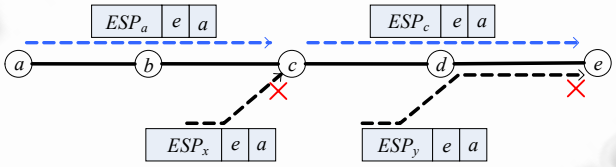


Fig.5 Portioning deployment of ESP

图 5 ESP 部分部署

3.4.2 动态路由

在动态路由过程中,从源节点到目的节点可能存在多条可行路径,源节点可以任意选择其中一条作为最佳路径.当最佳路径中链路失效时,可以改变最佳路径.当选择其他路径作为最佳路由后,根据 ESP 标识计算和通告算法可知,ESP 节点也将通过该最佳路径传递 ESP 标识和网络前缀,后续发送的报文能够在该路径中正确标记和过滤.可能发生节点立即向下游节点转发报文,而 ESP 标识的更新消息尚未到达下游节点,使得过滤表中标识与报文包含的标识不一致,被误判为 IP 欺骗的报文.但这只是更新延迟问题,是暂时的,影响很小.

4 性能评估

4.1 衡量标准

为了量化和评估 ESP 防御效果,引用文献[15]定义的防御性能衡量标准 $\phi_1(\tau)$和 $\phi_2(\tau)$,与 IDPF 进行比较.

定义 11(覆盖率). 网络实体中 ESP 节点所占比例,记为 γ.

定义 12(伪造的 IP 地址集合). 攻击者 a 攻击 t 时可以伪造的 IP 地址集合 $S_{a,t}$.利用 $S_{a,t}$ 中地址伪造报文源 IP 地址,该报文可以到达 t,不会被防御机制过滤.根据定义可知,$a \in S_{a,t}$.

定义 13(攻击者集合). 攻击 t 时能够伪造 s 中 IP 地址的攻击者集合 $C_{s,t}$.从这些节点中发送伪造 s 中的 IP 地址的报文攻击 t,在转发过程中不会被防御机制过滤.根据定义可知,$s \in C_{s,t}$.

$\phi_1(\tau)$从受害者 t 的角度描述过滤能力的衡量标准,任意攻击者能够伪造至多 τ 个 AS 中的 IP 地址攻击 t 的比例,表明了抵御欺骗 DoS 攻击的能力.

$$\phi_1(\tau)=\frac{|\{t:\forall a\in V,|S_{a,t}|\leqslant\tau\}|}{|V|},\tau\geqslant 1 \tag{3}$$

$\phi_2(\tau)$从攻击者 a 的角度描述过滤能力的衡量标准,能够伪造至多 τ 个 AS 中的 IP 地址的攻击者 a 的比例,表明了 ESP 防御机制对攻击者欺骗能力的限制.

$$\phi_2(\tau)=\frac{|\{a:\forall t\in V,|S_{a,t}|\leqslant\tau\}|}{|V|},\tau\geqslant 1 \tag{4}$$

4.2 模拟设置

我们基于 dpf2[15]实现了 ESP 防御机制模拟器.dpf2 由 3 个模块组成:cover,dpf 和 stats.cover 根据不同的输入规则,如随机选择、顶点覆盖(vertex cover)和排名顺序选择 ESP 节点.dpf 是主要模块,计算 $S_{a,t}$ 和 $C_{s,t}$,它的输入包括过滤类型和路由算法.stats 根据 dpf 的输出计算性能衡量标准.从 Oregon 大学的 RouteViews(University of Oregon Route Views Project,http://www.routeviews.org/)位于美国 ISC(isc.routeviews.org)、日本 DIXIE(wide.routeviews.org)和英国 LINX(linx.routeviews.org)的 3 个无缺省路由域 DFZ(default-free zone)中 BGP 路由器获得的 RIB,构造了 Internet 拓扑结构,分别记为 G_{usa},G_{japan} 和 G_{london}.表 1 总结了 3 个拓扑结构的属性.

Table 1 Properties of Internet topologies

表 1 Internet 拓扑结构属性

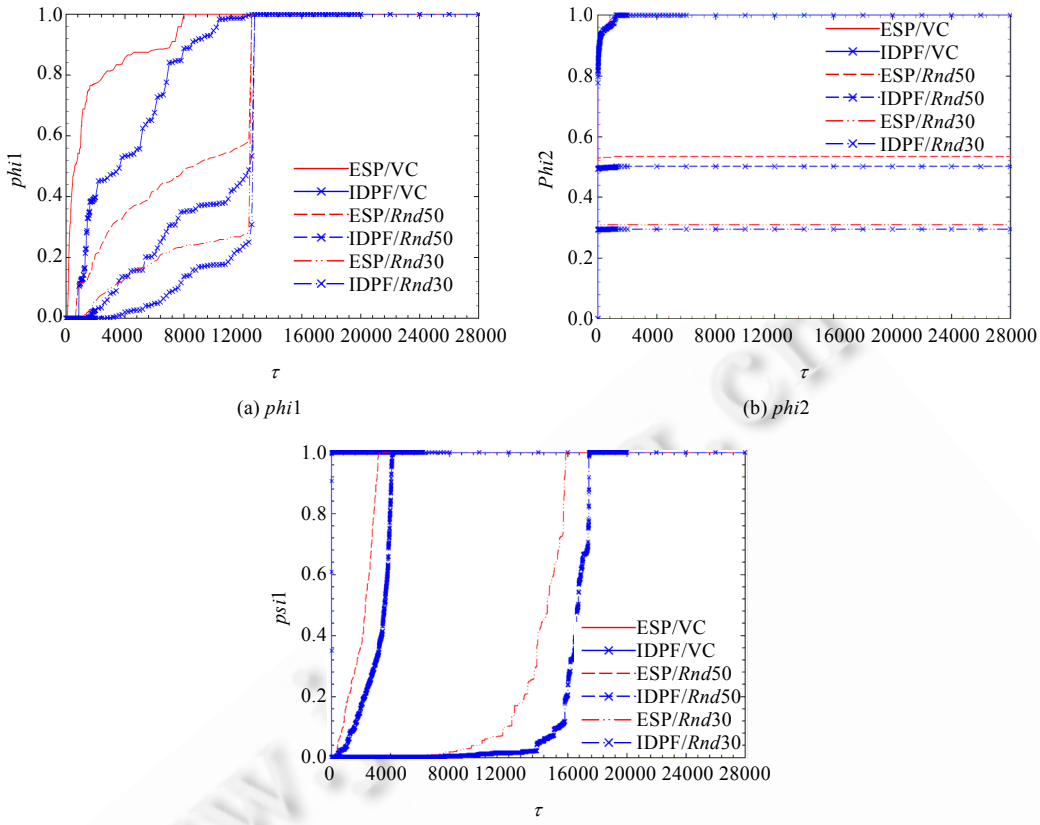
Graph	# of node	# of AS path	VC size
G_{usa}	28 018	9 154 266	3 954
G_{japan}	27 024	751 041	3 331
G_{london}	27 067	5 940 252	3 765

网络中,防御节点数和位置对 IP 欺骗防御机制的性能有一定的影响,因此,防御节点的选择也是关键.我们分析了随机选择防御节点,从网络节点中随机选取直到目标大小,如覆盖率为 30%和 50%,相应的防御节点集合记为 *Rnd*30 和 *Rnd*50;以及根据设计规则选取,如防御节点形成顶点覆盖.VC 覆盖了 Internet 结构中所有的边.

4.3 性能分析

从受害者角度分析 ESP 过滤能力.$\phi_1(\tau)$表示了可能受到攻击的节点 t 的比例.此时,攻击者能够伪造最多 τ 个节点的 IP 地址,其中,$\phi_1(1)$表示攻击者只能伪造最多 1 个 AS 的 IP 地址攻击 t,说明了 t 对欺骗攻击的免疫能力.图 6(a)表示了在 G_{usa} 中 3 种覆盖 *Rnd*30,*Rnd*50 和 VC 下 IDPF 和 ESP 的过滤能力.IDPF 不能完全防止 IDPF 节点受到欺骗攻击,$\phi_1(1)<\gamma$,除非网络中所有的节点支持 IDPF.而且,IDPF 节点的放置对于其性能有严重的影响,在 VC 下的性能超越了 *Rnd*30 和 *Rnd*50.在相同覆盖条件下,ESP 性能明显优于 IDPF.ESP 节点通过完整的 ESP 标识,能够过滤联盟成员发送的 IP 欺骗报文或非联盟成员伪造联盟成员 IP 地址的 IP 欺骗报文;而且根据 ESP 中路径标识,为邻居中非联盟成员提供了 IP 欺骗报文过滤服务,$\phi_1(1)>\gamma$.

从攻击者角度分析 ESP 过滤能力.$\phi_2(\tau)$表示了防御机制限制攻击者欺骗能力的效果,其中,$\phi_2(1)$描述了只能使用自己 IP 地址不能伪造其他 AS 的 IP 地址发起欺骗攻击的攻击者 a 的比例.图 6(b)表示了在 G_{japan} 中 3 种覆盖 *Rnd*30,*Rnd*50 和 *VC* 下 IDPF 和 ESP 的 $\phi_2(\tau)$值.IDPF 不能完全防止网络受到欺骗攻击,则突出对攻击者能力的限制.IDPF 在 *Rnd*30,*Rnd*50 和 VC 覆盖条件下,$\phi_2(1)$分别是 0.292,0.487 和 0.805.ESP 机制在相同配置下,$\phi_2(1)$分别是 0.324,0.517 和 0.839.由于 ESP 融合了源标识和路径标识,不仅能够在目的端过滤 IP 欺骗报文,而且能够在中间网络中提前过滤 IP 欺骗报文,性能明显优于 IDPF.



(a) *phi*1 (b) *phi*2

(c) *psi*1

Fig.6 Ability of filtering and tracing

图 6 过滤和追踪能力比较

4.4 部署激励

假设网络由 n 个节点(即自治域)组成,记为 $INT=\{1,2,\ldots,n\}$,支持 SPM(或 ESP)机制的节点记为 SPM(或 ESP).从 as_i 到 as_j 的攻击流流量记为 $A^k_{i\to j}$,其中,报文 IP 地址被伪造为 as_k 中的 IP 地址.SPM 机制能过滤的攻击流为

$$D_j^{SPM}=\sum_{k\in SPM}\sum_{i\in INT}A^k_{i\to j}+\sum_{k\in INT-SPM}\sum_{i\in SPM}A^k_{i\to j} \tag{5}$$

若部署 ESP,能够过滤任何节点发送的伪造 ESP 节点 IP 地址的攻击流,即 $\sum_{k\in ESP}\sum_{i\in INT}A^k_{i\to j}$;能够过滤 ESP 节点发送的伪造其他节点 IP 地址的攻击流,即 $\sum_{k\in INT-ESP}\sum_{i\in ESP}A^k_{i\to j}$;能够过滤 ESP 节点的邻居节点中非联盟成员 $i\in NN(ESP)$发送的伪造其他 ESP 节点的邻居节点中非联盟成员 IP 地址的攻击流,即 $\sum_{k\in NN(ESP)}\sum_{i\in NN(ESP)}A^k_{i\to j}$,是 $\sum_{k\in INT-ESP}\sum_{i\in INT-ESP}A^k_{i\to j}$ 的部分流量.ESP 机制能够过滤的攻击流至少为

$$D_j^{ESP}=\sum_{k\in ESP}\sum_{i\in INT}A^k_{i\to j}+\sum_{k\in INT-ESP}\sum_{i\in ESP}A^k_{i\to j}+\sum_{k\in NN(ESP)}\sum_{i\in NN(ESP)}A^k_{i\to j} \tag{6}$$

显然,在相同覆盖的情况下,即 $SPM=ESP$,ESP 机制能够过滤更多的非联盟成员发送的 IP 欺骗报文,即 $\sum_{k\in NN(ESP)}\sum_{i\in NN(ESP)}A^k_{i\to j}$,比 SPM 具有更高的部署激励.

5 总结和展望

IP 欺骗影响 Internet 的安全性和可用性,基于源-目的标识(密钥)的自治域级 IP 欺骗过滤和基于源标识(公钥)的端系统级 IP 认证均采用了端-端方式以试图解决 IP 欺骗防御问题.端-端认证方式实现简单,但却忽略了 IP 欺骗报文在网络中转发过程中所造成的破坏,防御效果差.ESP 是第一种面向 IP 欺骗防御联盟成员的域间 IP 欺骗防御服务增强机制.首先引入了开放的路由器协同机制,提供了源-目的路径中 ESP 节点信息通告和协同标记的框架;其次,基于源标识的 IP 欺骗防御,在源标识中融入了路径标识,减小了源标识冲突概率,而且混合型标识支持了 ESP 节点能够根据报文标识提前过滤 IP 欺骗报文;最后,基于域间路由协议 BGP,引入前缀 *p*-安全节点概念和检测理论,有效控制了源标识传播范围,能够减小 ESP 节点的标记和过滤开销.

ESP 继承了基于标识的防御机制的可部分部署性,能够很好地支持动态路由和非对称路由.应用 Routeview 提供的 RIB 进行评估,ESP 不仅增强了 IP 欺骗防御节点的能力,而且能够提前过滤 IP 欺骗报文.ESP 是一种高效的域间 IP 欺骗防御机制,为建设新一代可信网络提供了技术支撑.

未来会有更多的研究集中于如何将自治域级和端系统级 IP 欺骗防御机制相融合的方法.同时,IP 欺骗防御逐渐受到 IETF 的关注,我们相信,ESP 能够推动 IP 欺骗防御机制的标准化,这也是我们进一步研究的方向.

References:

[1] Hastings NE, McLean PA. TCP/IP spoofing fundamentals. In: Proc. of the 15th Annual Int'l Phoenix Conf. on Computers and Communications. IEEE Computer Society, 1996. 218−224. http://sciencestage.com/d/3840792/tcp/ip-spoofing-fundamentals.html

[2] Zhao X, Chen DX, Xie L. Study on IP Haijack. Journal of Software, 2000,11(4):515−519 (in Chinese with English abstract). http://www.jos.org.cn/ch/reader/view_abstract.aspx?flag=1&file_no=20000414&journal_id=jos

[3] Schuba CL, Krsul IV, Kuhn MG. Analysis of a denial of service attack on TCP. In: Proc. of the IEEE Symp. on. Security and Privacy. IEEE Computer Society, 1997. 208−223. http://cs.unc.edu/~fabian/course_papers/schuba.pdf

[4] Park K, Lee H. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law Internets. In: Proc. of the ACM SIGCOMM 2001. San Diego: ACM Press, 2001. 15−26. http://www.cs.purdue.edu/nsl/dpfsigcomm01.pdf

[5] Liu X, Yang XW, Wetherall D. Passport: Secure and adoptable source authentication. In: Proc. of the 5th USENIX NSDI. USENIX Association Press, 2008. http://www.seattle.intel-research.net/pubs/passport-nsdi.pdf

[6] David GA, Hari B, Nick F, Teemu K, Daekyeong M, Scott S. Accountable Internet protocol (AIP). In: Proc. of the ACM SIGCOMM 2008. Seattle: ACM Press, 2008. 339−350. http://www.cs.cmu.edu/~dga/papers/aip-sigcomm2008.pdf

[7] Ferguson P, Senie D. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. RFC 2267, Internet Engineering Task Force, 1998.

[8] Baker F. Requirements for IP version 4 routers. RFC 1812, Internet Engineering Task Force, 1995.

[9] Bremler-Barr A, Levy H. Spoofing prevention method. In: Proc. of the IEEE INFOCOM 2005. Miami: IEEE Press, 2005. 536−547. http://www.mnlab.cs.depaul.edu/seminar/spr2005/bremler05.pdf

[10] Yaar A, Perrig A, Song D. Pi: A path identification mechanism to defend against DDoS attacks. In: Proc. of the IEEE Symp. on Security and Privacy. IEEE Computer Society, 2003. 1−15. http://www.cs.berkeley.edu/~dawnsong/papers/pi.pdf

[11] Yaar A, Perrig A, Song D. StackPi: New packet marking and filtering mechanisms for DDoS and IP spoofing defense. Journal on Selected Areas in Communications, 2006,24(10):1853−1863.

[12] Li DQ, Su PR, Feng DG. Notes on packet marking for IP traceback. Journal of Software, 2004,15(2):250−258 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/15/250.htm

[13] Lee HJ, Kwon M, Hasker G, Perrig A. BASE: An incrementally deployable mechanism for viable IP spoofing prevention. In: Proc. of the ASIACCS 2007. Singapore: ACM Press, 2007. 20−31. http://portal.acm.org/citation.cfm?id=1229285.1229293

[14] Rekhter Y, Li T, Hares S. A border gateway protocol 4 (BGP-4). RFC 4271, Internet Engineering Task Force, 2006.

[15] Duan Z H, Yuan X, Chandrashekar J. Constructing inter-domain packet filters to control IP spoofing based on BGP updates. In: Proc. of the IEEE INFOCOM 2006. IEEE Press, 2006. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.69

[16] Krovetz T. Umac: Message authentication code using universal hashing. RFC 4418, Internet Engineering Task Force, 2006.

附中文参考文献:

[2] 赵欣,陈道蓄,谢立.网上 IP 劫持攻击的研究.软件学报,2000,11(4),515−519. http://www.jos.org.cn/ch/reader/view_abstract.aspx?flag=1&file_no=20000414&journal_id=jos

[12] 李德全,苏璞睿,冯登国.用于 IP 追踪的包标记的注记.软件学报,2004,15(2),250−258. http://www.jos.org.cn/1000-9825/15/250.htm

吕高锋(1980－),男,陕西扶风人,博士,助理研究员,主要研究领域为高性能路由与交换技术,高可信网络.

孙志刚(1973－),男,博士,副研究员,CCF 高级会员,主要研究领域为高性能路由器,新型网络体系结构.

卢锡城(1946－),男,教授,博士生导师,中国工程院院士,CCF 高级会员,主要研究领域为分布处理技术,计算机网络与通信技术.