专题:高可信网络与网络安全

互联网中IP源地址伪造及防护技术*

姚 广,毕 军

(清华大学信息网络工程研究中心 北京 100084)

摘 要 当前的互联网上出现了越来越多地使用伪造源地址发起网络攻击的行为。这种攻击行为容易发动且难以被追查出,如何降低攻击带来的危害,制止攻击的发生和追查攻击者真实身份成为一个重要问题。本文总结了伪造源地址攻击的攻击方式,并分析了现有的伪造源地址防御技术。

关键词 伪造源地址;互联网;防护

1 引言

随着互联网使用环境的变化,互联网技术的缺陷正逐渐暴露出来,其中不保证源地址的真实性便是一个重要问题。互联网之初主要用于学术目的,当时假设网络中的所有设备都是可信任的,因此报文在转发过程中没有认证源地址的真实性。而在当前复杂的互联网环境下,这种网络设备普遍可信的情况早已不复存在,与之相反,每一台设备都可能伪造其源地址来达成特殊目的。当今,通过伪造源地址来辅助发起网络攻击的行为十分频繁。据统计,一周内借助伪造源地址发起的DoS攻击至少有4 000起。因此,保证报文中源地址的真实性成为当前急需解决的问题。

2 伪造源地址及真实地址问题的定义

为了在互联网中进行正常的通信,报文的发送方必须在发送的报文的源地址字段填写分配给发送方的真实IP地址[1],这样报文的接收方才知道将回复发往哪一个地址。出于某种特殊目的,报文的发送方将报文中携带的源地址修改为任意地址,这种行为称为伪造源地址。由于当前的互联网没有完全部署对使用伪造源地址的报文进行过滤的机制,并且路由器对报文的转发只是基于报文的目的地址,这些报文一般情况下可以正常到达目的地,因此通过伪造报文源地址可以发起某些网络攻击行为。因为难以发现伪造源地址报文的真实源头,所以在攻击发生之后很难追查出真正的攻击者。伪造源地址的攻击容易被发动却难以被追查的特点,使得这类攻击在互联网上极为普遍。解决源地址伪造,保证报文中源地址的真实性,就是所说的真实地址问题。

3 伪造源地址攻击的类型

并不是所有的伪造源地址行为都能够构成攻击。单纯的、不以攻击为目的的伪造源地址行为对互联网的危害是很微小的,但是伪造源地址被用来发起攻击,则有可能产生巨大的危害。确定伪造源地址的攻击类型有助于更加清晰地了解真实地址问题。按照攻击者伪造地址的不同和受害者的不同,可以将伪造源地址攻击分为以下3类。

* 国家"973"计划(No.2003CB314801)和国家科技支撑计划"可信任互联网"资助项目

(1) 伪造随机的源地址,受害者是报文的接收方

攻击者通过伪造源地址的方式大量占用受害者的预留资源,使受害者无法正常为其他用户提供服务,称为DoS[2]攻击。除非报文接收端对报文的处理代价很高或者接收端的链路带宽很小,否则单纯的伪造源地址的DoS攻击无法直接充分占用受害者的带宽资源或者处理能力,因为单一或者少数设备并不能产生足够使受害者的链路饱和或者超出目标设备处理能力的伪造源地址流量,而只能占用一些特定的资源。最常见的DoS攻击为SYN flooding[3]攻击。

DDoS[4]攻击是DoS攻击的一种特殊方式,攻击者通过某些方式控制大量的主机,这些主机同时向受害者发送大量报文,完全占用受害者的通信链路或资源,使受害者无法向其他用户提供正常服务。对于这种攻击,较好的处理方法是通知上游网关屏蔽来自相应地址的流量[5]。但是,如果DDoS同时辅以伪造源地址的手段,就会使受害主机无法判断攻击者的真实来源,从而无法在邻近网关上进行过滤。在这种情况下,攻击是无法被直接消除的,除非有办法识别并且过滤掉伪造源地址的攻击流量。

(2)伪造特定的源地址,受害者是伪造报文的接收者

攻击者通过伪造具有特定源地址的报文,使受害者接收某些虚假信息。在互联网中一些机制将报文的源地址作为认证的惟一手段,只要攻击者在网络中插入精心设计的报文,在没有安全保护策略的情况下,这些报文都有可能被接收端相信,而做出攻击者希望的响应。攻击者对被攻击者的回复报文可能是可见的,也可能是不可见的,但是攻击者可以猜测出回复的内容。最典型的攻击方式是中间人攻击[6]。

攻击者一般会伪造网络中重要设备的通信报文,例如关键路由器路由更新、DNS服务器的信息交换、邮件服务器交换的电子邮件等,然后向其他设备散布符合自己目的的虚假信息。伪造路由信息造成路由转向是一种常见的攻击方式,参考文献[7]描述了在路由器之间散布虚假路由的情况。

(3)伪造特定的源地址,受害者是被伪造者

DrDoS[8]是一种特别的DDoS攻击,攻击者向大量的主机发送伪造源地址的某种请求回复的报文,这些报文的源地址被设置为受害者的地址,这样大量的回复被"返回"给受害者,饱和其链路或者使其过载,达到和DDoS攻击相同的效果。参考文献[9]描述了一个典型的利用DNS服务器的DrDoS攻击。对于这类攻击,受害者无法直接屏蔽这些主机(因为它们并非是恶意的攻击者),只有通过过滤伪造源地址的报文来制止。最典型的攻击方式是Smurf攻击[10]。

此外,由于IP地址在互联网络是设备和用户身份的象征,因此攻击者可以通过伪造受害者的IP地址在网络中进行一些不法行为,例如抢占带宽、攻击某些设备等,一旦这些行为触及运营商或其他服务提供商的管理规则,则有可能导致受害者的利益或者名誉受损。

4 伪造源地址防御技术

4.1 实现方案

伪造源地址防御方案(即真实地址问题解决方案)按照工作方式的不同可以分为路径上过滤、端到端和Traceback 3类。

4.1.1 路径上过滤方案

顾名思义,路径上过滤就是对伪造源地址的报文的检查和过滤发生在报文传播的路径上,也就是在伪造源地址的报文到达目的地之前过滤掉这些报文。路径的中间节点具有检查报文真实性的能力,不过对报文的过滤也可能发生在报文的接收端。中间节点具有检查能力是路径上过滤方案与端到端方案的不同之处。由于可以在报文的传播路径上进行过滤,因此这类方案可以在伪造报文到达受害者之前将其清除,使受害者完全或者很大程度上避免接触攻击报文,具有非常好的保护效果,尤其对DoS攻击具有很好的防御作用。但是,由于使用了与路径相关的信息,因此在路由不稳定的情况下可能会将正确的报文丢弃。这类方案的典型代表有Ingress Filtering[11]、DPF[12]、SAVE[13]、Passports[14]、HCF[15](hop count filtering)和ARBIF[16]等。另外,在接入网的接入处限制接入网内的机器伪造源地址的方案也属于路径上过滤方案。

(1)Ingress Filtering

Ingress Filtering部署在两个网络连接处的路由器或者防火墙中,由该路由器或者防火墙负责检查来自这个网络的报文的源地址是否属于这个网络。如图1所示,路由器只允许向外转发地址前缀是202.112.68.*的报文,对于其他源地址的报文将丢弃。RFC 2827给出了Ingress Filtering的定义,并规定被检查的网络限定为ISP的接入网络。RFC 3704给出了Ingress Filtering的5种实现方式,其中包括手动和自动配置方式以及满足Multi-homing和非对称路由情况的实现方式。Ingress Filtering的自动配置主要利用了路由转发的uRPF[17]特性。

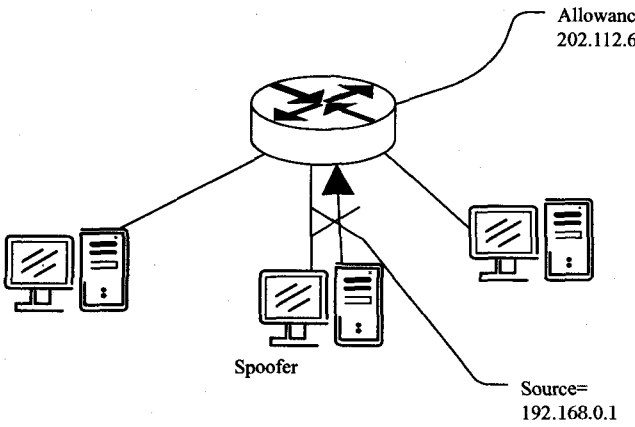

图 1 Ingress Filtering 实现原理示意

Ingress Filtering 是最有效且轻量的过滤方案，它可以使所有伪造源地址的报文不能离开攻击者所属的子网,而且只需要使用路由器中最基本的数据结构。如果所有的接入网络都部署 Ingress Filtering，那么伪造源地址的攻击就不可能被发起。

普遍认为 Ingress Filtering 是一种“自律性”的真实地址方案,而不是防御性方案。按照 RFC 2827 给出的方式部署,它将无法防范任何来自外界的伪造源地址的攻击，只是可以制止内部网络发起这类攻击。对于网络运营商而言,这样部署 Ingress Filtering 是没有任何好处的，因而没有被广泛采用。但是,认为 Ingress Filtering 完全没有防御能力是一种错误的认识。Ingress Filtering 只能部署在接入子网与 ISP 的连接处的限制是不必要的,ISP 网络与 ISP 网络之间的连接处也可以部署 Ingress Filtering,只是配置更加复杂。当一个 ISP 使用 Ingress Filtering 来处理来自另一个 ISP 的报文时,它将得到一定的保护。但是,ISP 地址分配和路由选择的复杂性,使 Ingress Filtering 的实用性受到限制。

(2)DPF

DPF 根据路由信息和网络拓扑信息来判断到达一个路由器的报文是否拥有合法的地址,因为从某个源地址去往某个目的地址的报文到达该路由器经过的链路是一定的。如图 2 所示,A 事先知道来自于 B 的报文只会从固定的接口到达,D 伪造的 B 报文被发现从另外一个接口到达,A 根据源地址和接口的对应关系过滤掉 D 的伪造报文。

DPF 也是一种轻量方案，过滤报文增加的负荷接近于一次或两次路由查找的负荷。单个路由器部署 DPF,过滤效果有限,因为一个路由器只和较少的链路相连。如果 DPF 被广泛部署,过滤作用将很明显。如果 18%的网络部署 DPF,则可以减少 90%的伪造源地址攻击报文。

DPF 主要的缺点是无法处理攻击者伪造同一反向路径上的其他主机地址的行为。在这个反向路径特别巨大的情况下,DPF 的过滤能力就会十分弱。

DPF 需要的报文到达本地的链路信息从现有路由器中是无法获取的。在对称路由情况下,uRPF 特性可以被用来获取这些信息；在非对称路由情况下,只能通过辅助的协议来获取这些信息。BGP Route Selection Notice[18]是由清华大学提出的一种域间的基于 BGP 的 DPF 方案。在该方案中,当一个 BGP 路由被选择时,其他的路由器将被通知,使得这些路由器可以获知来自某个源地址的报文到达本地路由器经过的链路,这样就能够执行 DPF 中对报文源地址真实性的检查。

(3)SAVE

SAVE 是一种在自治域的边界路由器上建立到达本地的报文源地址和接口对应关系的协议。在 SAVE 协议中,边界路由器之间相互交换路由表信息,并将收到的路由信息映射到接收到这个信息的接口,以获取正确的源地址—接口对应表。SAVE 协议面对的是非对称路由下的需求,事实上可以作为 DPF 在非对称路由下的辅助协议。

SAVE 较好地解决了非对称路由下的伪造源地址过滤问题,但是它依然无法解决在攻击者伪造同一反向路径上源地址问题。SAVE 存在的另一个问题是,参与协议的路由器必须进行大量的、可认证的数据交换,不但复杂性比较高,而且这个过程可能成为 DoS 攻击的对象。SAVE 协议需要全局部署之后才能发挥作用，因为在全局部署之前,源地址—接口对应表并不说明某个接口只能收到相应源地址的报文,而只是说明这个接口可能收到来自这些源地址的报文,即这个表不能用来过滤。不能增量部署限制了它的推广应用。

(4)Passports

Passports 是一种在报文中添加报文所需要经过的全部

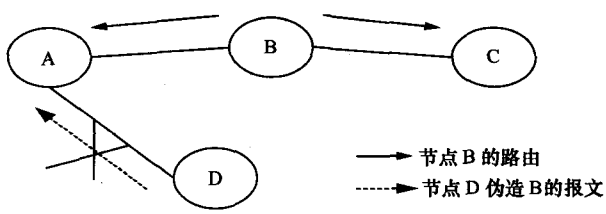

图 2 DPF 实现原理示意

自治域要检查的签名的方法。如图 3 所示,当自治域 AS1 的主机向自治域 AS4 的主机发送报文时,在 AS1 的出口网关处,报文被添加上路径中自治域 AS2、AS3、AS4 各自所需要检查的签名,在这个报文所路经的自治域边界处,相应的签名的正确性都会被检查,一旦发现对应的签名不正确或者不存在,则认为是伪造源地址的报文而被丢弃。

Passports 与其他路径上过滤方案相比,最大的特点是使用了密码学手段来认证源地址的真实性;而与其他使用密码学手段的方法相比,例如 IPSec,最大的优点在于可以将伪造流量在到达受害者之前过滤掉。Passports 最大的缺点是在报文中增加了过多的负荷。每一个用于认证的签名的长度达 64 位,如果报文需要通过多个自治域,整个签名部分的长度非常长,而且对这些签名验证的代价也会增加。

(5)HCF

HCF 是一种基于报文中的 TTL 来判断报文是否使用伪造源地址的方法。每收到一个报文,可以通过其中的 TTL 值猜测报文最初被赋予的 TTL 值,进而得到报文到达本地所经过的跳数,将这个跳数与事先得到的相应前缀到达本地的跳数对比,如果出现很大的偏差,就可以认为这个地址是伪造的。这种方法的依据是,伪造源地址的报文一般不会伪造出正确的 TTL 值,只要网关可以获知属于这个源地址的大概的 TTL 范围,那么就可以过滤掉 TTL 明显不对的报文。在参考文献[19]中详细描述了这种方法的一个应用。

HCF 也是一种轻量方案,只增加一次路由查找的负荷,就能过滤掉接近 90%的伪造源地址报文。但是,在攻击很严重的情况下,剩余的 10%流量也可以造成严重的攻击,而且如果攻击者事先进行探测,就可能伪造出正确的 TTL 值,这样 HCF 会被绕过而完全不起作用。HCF 的另外一个缺陷是,从 IP 地址前缀到跳数的映射表的获取是很复杂的,这个过程还很容易被攻击。

(6)ARBIF

ARBIF 是一种利用自治域之间的邻接关系来判断源地址真实性的方法。它主要依赖于邻接的自治域直接信赖关系的传递性来对源地址进行认证。ARBIF 需要预先知道网络的拓扑,在此基础上建立信任关系。

ARBIF 过滤的代价接近于一次或两次路由查找的代价,是一种很轻量的方法。在部署较好的情况下,ARBIF 可以达到很好的域间过滤效果。ARBIF 的问题是不够灵活,需要基于很多不能自动发现的信息来产生过滤规则,增加 ARBIF 的灵活性是一个值得研究的方向。另外,ARBIF 应对路由变化的机制还在进一步研究之中。

(7)接入网过滤方法

在路径上过滤这类方案中,有一些方法具有比较类似的特性:它们一般部署在距离主机最近的网关上,目的是检验本地主机发出的报文的源地址的真实性,对来自外界的攻击没有防范能力。这些方法被单列为一类,称为接入网过滤方法。这类方法是出于部署者的一种自我约束的需求产生的,往往部署在最靠近主机的地方,目的是防止这些主机伪造其他地址,但是没有防御外来的伪造报文攻击的能力。这些方法包括 DHCP Lease Query[20]、Signature-based Authentication[21]、IP Source Guard[22]、Ethane[23]、NAC[24]、TNC[25]、NAP[26]。Ingress Filtering 可以作为接入网过滤方法的一个选择,但是它并不是专用于接入网过滤,所以并不归属于这个类别。

4.1.2 端到端方案

端到端方案使报文的接收端在获取报文时能够获知报文源地址的真实性,即在报文的发送端报文添加签名,报文的接收端根据这个签名来判断报文源地址的真伪性,在中间网络上不判别报文源地址的真实性。报文的接收端可能是各种粒度的,可以是一个自治域,也可以是一台主机。端到端方案并不一定用于制止带有伪造源地址的 DDoS 攻击,还可能用于需要确保源地址真实性的应用需求。这类方案的典型代表有 IPSec[27]、SPM[28]和 APPA[29]等。

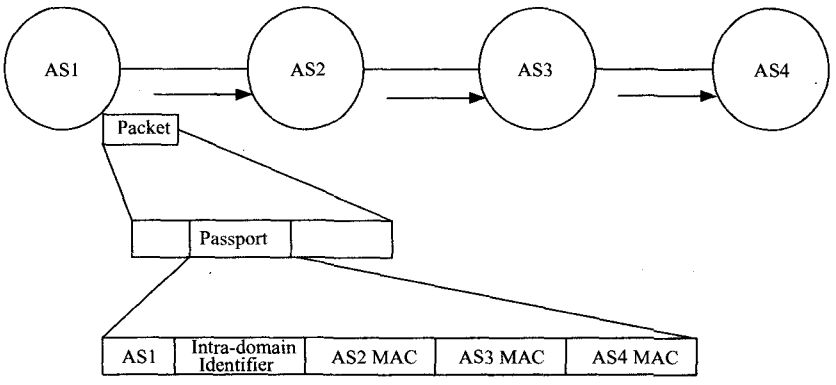

图 3 Passports 实现原理示意

(1)IPSec

IPSec是主机级别的端到端真实地址方案。RFC 2401~2409中详细定义了IPSec的相关技术。IPSec采用私钥签名方式进行认证。在发送的报文中增加一个认证头AH(AH是对整个报文内容和源地址的一个私钥加密的结果),报文的接收方使用发送方的公钥解密AH,就可以得知报文的源地址是否真实。AH头同时还能用于防止重放攻击和验证报文完整性。但是,这种认证方式的网络开销较高,使得IPSec不但无法防止DDoS攻击,而且很有可能成为DDoS攻击的对象。

IPSec是目前保护粒度最高的认证机制,在强制部署的情况下,它可以使一台主机无法伪造其他主机的地址与别的主机进行通信。

(2)SPM

SPM是一种域间真实地址方案,采用签名—认证验证体系。当报文离开自治域时,自治域的网关路由器将为其添加一个基于源—目的的自治域对的签名,当到达目的自治域时,将检查这个签名,没有签名或者含有错误签名的报文将被丢弃。

SPM没有采用任何加密技术,因此整个方案比较轻量,验证代价接近于一次路由表查找的代价。SPM的保护粒度是一个自治域,即一个自治域内主机的源地址不能被其他自治域的主机伪造。由于验证的轻量性和边界路由器的强大性能,因此SPM不会成为DDoS的攻击对象。

SPM的安全性是基于主干网的报文难以被窃听这一前提的。但是,主干网的报文难以保证不被窃听,特别是在报文穿越自治域时,签名被窃取的可能性很大,一旦签名被窃取,攻击者就可以伪造出具有正确签名的报文。另外,SPM的签名发布和更新过程也可能成为攻击对象。签名发布有主动和被动两种方式。网络中自治域较多,主动交互的高代价可能引来DoS攻击;被动的签名发布存在被攻击者欺骗的可能性。签名的更新有主动散布和使用伪随机数两种方式,前者存在大规模应用更新频率可能无法满足要求的问题,后者在同步上缺乏验证。

(3)APPA

APPA类似于SPM,都使用双方共享的签名来对报文源地址的真实性进行认证。APPA的特点在于通信双方共同使用一个单向的Hash函数来自发计算通信的签名,而不是采用交互的方式。这样的好处是:减少了通信双方的交互,降低了复杂性,避免了交互带来的安全问题。APPA所采用的产生签名方式可以快速生成下一个签名,可以做到一个签名只使用一次,在这种情况下,签名即便被窃听,攻击者也无法使用这个签名伪装成APPA的部署者,所以APPA在安全性上比SPM要高。

互联网上的IP报文存在的乱序问题增加了一次一密情况下APPA验证的复杂性。APPA正在进行进一步的完善以处理这些细节问题。

4.2 Traceback类方案

Traceback类方案没有直接的保护作用,但是可以追查攻击者的真实位置,进而采用其他方法来消除攻击。Traceback类方案主要采用报文标记、路由器记录以及收集器处理等方式来确定报文的来源。

(1)报文标记

在报文中加入路由器的标记,报文的接收者可以根据这些标记来判断报文所经过的实际路径。采用报文标记方式的Traceback方案有PPM[30]、DPM[31]、Pi[32]和AITF[33]。

这种实现方式不会给路由器增加太大的负担,路径的确定算法也很轻量。它的问题在于,经过的路由器越多,加入的标记就越多,报文长度会越长,或者以前的标记被清除掉。因此,报文标记Traceback方案不适合大型网络。

(2)路由器记录

每一个路由器保存一张位图,路由器利用Hash函数将转发的报文转换成一个数字,这个数字对应位图上的相应位,该位将被标记,一旦管理者发现需要追查某个报文的源头,他会向所有的路由器发出请求以获取标记了相应位的路由器信息,进而可以找到报文被转发的路线。采用这种实现方式的Traceback方案典型代表有Hash-based IP Traceback[34]。

这种实现方式占用的空间和消耗的时间都是相当轻量的。其最大的问题就是Hash碰撞,不同的报文可能Hash到相同的位上,导致追查时无法辨别。在高速网络中,报文的数量很多,碰撞的次数会相应增加,这个问题更加严重。

(3)收集器处理

利用一个收集器处理来自路由器的报文或者消息,根据收集器获得的信息确定报文的路径。采用这种实现方式的Traceback方案代表有iTrace[35]和CenterTrack[36]等。这种实现方式给路由器造成的负担是最小的,因为路由器不必进行标记或者记录,只需要转发特定的报文。但是,收集器容易成为网络的瓶颈。

4.3 方案比较

表1从几个方面对路径上过滤和端到端两类方案的

代表技术做了比较。Traceback 类方案都没有主动防御能力,因此这里不考虑。同时,考虑到全局部署难度比较大,所以这里只考虑非全局部署。

RS 为 random source 缩写, FS 为 fixed source 缩写, RD 为 random destination 缩写, FD 为 fixed destination 缩写。

从以上的分析可以看出,当前各种方法本身都存在一定的问题, 没有一种方法可以完美解决源地址伪造问题。尽管完全部署 Ingress Filtering 是一种技术上最为简单且有效的方法,但是缺少激励机制,导致它无法被完全部署。DPF 是一种更加实际的替代方案,目前正在对 DPF 进行补充和强化。在端到端过滤机制中,SPM 指出了一个值得进一步研究的方向,尽管这个方案本身存在一些漏洞,但是后继 APPA 的发展能弥补其不足,它的轻量可能会使它在路由器中被广泛采用。Passports 的提前过滤特性值得进一步的研究。在上述方法中,IPSec 的验证代价最大,其他方法在认证上都很轻量。IPSec 的认证代价使得它在高速网络中很难应用。IPSec 可以作为专门应付第二类攻击的补充机制。

5 结束语

伪造源地址发起攻击的行为在互联网上日益猖獗。借助于伪造源地址, 攻击者可以发起危害极大的 DDoS 攻击,除此之外,还可以进行诋毁、散步虚假信息等攻击。为了减轻此类攻击的危害,必须过滤伪造源地址的报文,保证报文源地址的真实性。现有的伪造源地址防御技术并不能完美解决真实地址问题,但是对其中一些方案进行改进则有可能接近最终目标,这些方案的进一步改善将成为将来的研究方向。除此之外,希望能够建立起保证源地址真实性的互联网体系结构,从根本上解决源地址伪造问题。

参考文献

1 Heberlein L T, Bishop M. Attack class: address spoofing. In:Natl Information Systems Security Conf, 1996: 371~378

2 Garber L. Denial-of-service attacks rip the Internet. Computer, 2000,33(4):12~17

3 Computer emergency response team (CERT). TCP SYN flooding and IP spoofing attacks. Technical Report CA-96:21, Carnegie Mellon University Pittsburgh, PA, Sept 1996

4 Elliott J. Distributed denial of service attack and the zombie ant effect. IT Professional, 2000(3/4): 55~57

5 Yu Chen, Yu-Kwong Kwok, Kai Hwang, MAFIC: adaptive packet dropping for cutting malicious flows to push back DDoS attacks. ICDCS Workshops, 2005

6 Definition of man-in-the-middle, http://www.wordspy.com/words/maninthemiddleattack.asp

7 Huang Dijiang, Cao Qing, Sinha A, *et al*. New Architecture for Intra-Domain Network. Communication of the ACM, 2006,49(11)

8 Gibson S. Distributed reflection denial of service: description and analysis of a potent, increasing prevalent, and worrisome internet attack. http://grc.com/dos/drdos.htm , Feb 2002

9 SSAC advisory SAC008 DNS distributed denial of service (DDoS) attacks. A Report from the ICANN Security and Stability Advisory Committee (SSAC) , March 2006

10 CERT Advisory CA-1998-01 Smurf IP Denial-of-Service Attacks, http://www/cert.org/advisories/CA-1998-01.html, January 1998

表 1 各种方法对攻击方式的防御能力

方法 \ 攻击方式	RS,FD	FS,FD	FS,RD
Ingress Filtering	无明显效果	无效果	无效果
DPF	明显,可以过滤大量的攻击报文	可能失效(反向路径问题)	可能失效(反向路径问题)
SAVE	非全局部署则失效	非全局部署则失效	非全局部署则失效
Passports	对于域间情况, 具有很好的过滤效果,且能够做到提前过滤	对于域间情况,可以保护部署者	对于域间情况,可以保护部署者
HCF	效果明显,但是可能被绕过	在攻击者和被伪造者具有同样跳数的情况下可能失效	在攻击者和被伪造者具有同样跳数的情况下可能失效
ARBIF	域间效果明显,且能够做到提前过滤	域间情况一定程度可以保护部署者	域间情况一定程度保护部署者
IPSec	可能成为被攻击的对象,从而形成瓶颈	保证主机级别的认证能力	保证部署者名誉不受损害
SPM	域间效果明显,但是不能提前过滤	域间情况可以保护部署者	域间情况可以保护部署者
APPA	域间效果明显,但是不能提前过滤	域间情况可以保护部署者	域间情况可以保护部署者

11 Ferguson P, Senie D. Network ingress filtering: defeating denial of service attacks which employ IP source address spoofing. RFC 2267,May 2000

12 Park K, Lee H. On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets. In: ACM SIGCOMM 2001, San Diego, CA, USA, August 2001

13 Li J, Mirkovic J, Wang M, *et al*. SAVE: source address validity enforcement protocol. In: INFOCOM 2002, June 2002

14 Liu Xin, Yang Xiaowei, David W, *et al*. Efficient and secure source authentication with packet passports. In: SRUTI' 06, San Jose, CA, USA, 2006

15 Jin G, Wang H, Shin K G. Hop-count filtering: an effective defense against spoofed DDoS traffic. In :Proceedings of the 10th ACM conference on Computer and communication security, Washington DC, USA, 2003

16 Wu Jianping, Ren Gang, Li Xing. Source address validation: architechture and protocol design. In:ICNP 2007, Beijing, China, Oct 2007

17 Unicast reverse path forwarding. Cisco IOS, 1999

18 Wang Lijun, Xu Ke, Wu Jianping. BGP route selection notice. In: ICOIN 2006, Sendai, Japan, Jan 2006

19 Pazi G, Barr A B, Rivlin R, *et al*. Protecting against distributed denial of service attacks. Patent Application 20030110274

20 Woundy R, Kinnear K. Dynamic host configuration protocol (DHCP) leasequery, http://www.ietf.org/rfc/rfc4388.txt

21 Xie Lizhong, Bi Jun, Wu Jianping. An authentication based source address spoofing prevention method deployed in IPv6 edge network. Lecture Notes in Computer Science, 2007 (4490) : 801~808

22 Baker F. IP Source Guard,draft-baker-sava-cisco-ip-source-guard-00. txt, www. ietf. org

23 Casado M, Freedman J M, Pettit J, *et al*. Ethane: Taking control of the enterprise. In:ACM SIGCOMM 07, Kyoto, Japan, 2007

24 NAC, http://www. cisco. com/en/US/netsol/ns617/networking_solutions_ sub_solution_home. html

25 TCG trusted network connect TNC architecture for interoperability. TCG published

26 NAP, http://www.microsoft.com/technet/network/nap/default.mspx

27 Kent S, Atkinson R. Security architecture for the internet protocol. RFC 2401, 1998

28 B-B A, L H. Spoofing prevention method. In: IEEE Infocom, 2005

29 Shen Yan, Bi Jun, WuJianping, *et al*. A Two-level spoofing prevention method. In: ICC 2007,Glasgow, Scotland, June 2007

30 Savage S, Wetherall D, Karlin A, *et al*. Practical network support for IP traceback. In: ACM SIGCOMM, 2000: 295~306

31 Belenky A, Ansari N. IP traceback with deterministic packet marking. IEEE Communications Letters, 2003,7(4)

32 Yaar A, Perrig A, Song D. Pi:a path identification mechanism to defend against DDoS attacks. In: Proc IEEE Symp Security and Privacy, 2004

33 Argyraki K, Cheriton D. Active internet traffic filtering: real-time response to denial-of-service attacks. In:USENIX 2005, Anaheim, CA, USA, 2005

34 Snoeren C A, Partridge C, Luis A S, *et al*. Hash-based IP traceback. In: Proc of the ACM SIGCOMM 2001, San Diego, CA, USA, August 2001

35 Bellovin S, Leech D, Taylor T. Icmp traceback messages, http://www.ietf.org/internet-drafts/draft-ietf-itrace-04.txt, February 2003

36 Stone R. CenterTrack: an IP overlay network for tracking DoS floods. In: USENIX Security Symposium 2000,Denver, CO, August 2000

Source Address Spoofing and Prevention Technologies in Internet

Yao Guang, Bi Jun

(Network Research Center, Tsinghua University, Beijing 100084, China)

Abstract Nowadays more and more attacks on Internet exploit IP spoofing technology. This kind of attacks is easy to launch and hard to trace. How to reduce the damage of such attacks, prevent them from happening and trace the actual location of the attackers has been a crucial problem. This document conclude the mode of IP spoofing attacks, and analyse the existing anti-spoofing mechanisms.

Key words source address spoofing, internet, prevention

(收稿日期:2007-12-20)