软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2018,29(1):176−195 [doi: 10.13328/j.cnki.jos.005318]

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

互联网自治域间 IP 源地址验证技术综述*

贾溢豪[1,2,3], 任 罡[2,3], 刘 莹[2,3]

[1](清华大学 计算机科学与技术系,北京 100084)

[2](清华信息科学与技术国家实验室(清华大学),北京 100084)

[3](清华大学 网络科学与网络空间研究院,北京 100084)

通讯作者: 刘莹, E-mail: liuying@cernet.edu.cn

摘 要: 当前,互联网是基于目的地址转发,对源地址不作验证.而互联网很多安全问题的根源在于源地址的不可信.另一方面,随着互联网规模和复杂度的增大以及对政治、经济利益影响的加深,域间路由系统对互联网的稳定运行起着愈发关键的作用.美国国土安全部将域间路由安全问题列入了美国信息安全的国家战略.近年来,以 IP 源地址伪造为主要方式的分布式拒绝服务攻击不断地对互联网的安全性和可用性造成极大的破坏,这其中,以跨越多个管理域和国家的攻击最为频繁.因此,建立以自治域为单位的源地址验证防御体系,对互联网的安全意义重大.尽管在相关的标准和研究领域已经提出了多种域间源地址验证技术,但是目前仍未有适用于大规模部署的技术方案.对域间源地址验证的已有研究和标准进展进行了细致的梳理.首先,分析了源地址安全性缺失的原因及后果,结合国际标准化领域的研究现状,指出了域间源地址验证的重要意义;其次,从域间源地址验证技术的特征类别入手,对已有各类研究成果的技术原理和优缺点进行了深入的总结,对研究的演进脉络进行了详细的分析,并在此基础上提出了目前域间源地址验证技术面临的困境及原因;最后,提出了域间源地址验证技术未来可能的研究发展方向及设计原则建议,为后续相关研究工作的开展提供了参考.

关键词: 自治域间;IP 源地址验证;网络安全;分布式拒绝服务攻击

中图法分类号: TP393

中文引用格式: 贾溢豪,任罡,刘莹.互联网自治域间 IP 源地址验证技术综述.软件学报,2018,29(1):176−195. http://www.jos.org.cn/1000-9825/5318.htm

英文引用格式: Jia YH, Ren G, Liu Y. Review of Internet inter-domain IP source address validation technology. Ruan Jian Xue Bao/ Journal of Software, 2018,29(1):176−195 (in Chinese). http://www.jos.org.cn/1000-9825/5318.htm

Review of Internet Inter-Domain IP Source Address Validation Technology

JIA Yi-Hao[1,2,3], REN Gang[2,3], LIU Ying[2,3]

[1](Department of Computer Science and Technology, Tsinghua University, Beijing 100084, China)

[2](Tsinghua National Laboratory for Information Science and Technology (Tsinghua University), Beijing 100084, China)

[3](Institute for Network Sciences and Cyberspace, Tsinghua University, Beijing 100084, China)

Abstract: The current Internet is based on the destination address forwarding in which the source address remains unverified. However, one of the root causes of Internet security problems is the untrustworthy source address. As the Internet plays an increasingly important role in political and economic fields, the security of the Inter-domain Internet becomes more crucial. For instance, the US Department of

* 基金项目: 国家自然科学基金(61772307, 61402257); 国家重点基础研究发展计划(973)(2009CB320500, 2009CB320501); 清华大学自主科研项目(2014z21051)

Foundation item: National Natural Science Foundation of China (61772307, 61402257); National Basic Research Program of China (973) (2009CB320500, 2009CB320501); Tsinghua University Self-Determined Project (2014z21051)

收稿时间: 2016-03-16; 修改时间: 2017-03-27; 采用时间: 2017-06-14; jos 在线出版时间: 2017-07-12

CNKI 网络优先出版: 2017-07-12 16:16:52, http://kns.cnki.net/kcms/detail/11.2560.TP.20170712.1616.016.html

Homeland Security (DHS) has included the Inter-domain routing security in the national strategy of US information security. In recent years, innovation and evolution of the Internet are significantly undermined by the IP spoofing based distributed denial of service attacks, most of which are Inter-domain and transnational. Therefore, the Inter-domain source address validation becomes extremely important for Internet security. Although there are many techniques proposed in the relevant fields, none of them are appropriate for large-scale deployment. This paper reviews the existing research and standard progress of Inter-domain source address validation technology. First, the reasons and consequences of the lack of source address security are analyzed, and the significance of source address validation is illustrated by examining the progress of the technical standardization. Next, the advantages and disadvantages of various existing important source address validation methods are summarized. Then, the difficulties and challenges faced by the current Inter-domain source address validation technology are discussed. Finally, the prospective research directions and design principles are proposed as a reference for potential future works.

Key words: inter-domain; IP source address validation; Internet security; distributed denial of service attacks

互联网作为全球信息化基础设施,对世界各国政治、经济、文化、社会生活和国家安全等方面产生重大影响,已成为重要的国家战略资源.网络空间作为继陆、海、空和太空之后的人类第五疆域,获得了世界各国的高度重视.然而,由于互联网设计之初没有充分考虑网络成员不可信带来的安全威胁,网络体系结构本身存在安全设计缺陷,这使得网络的安全可信面临极大的挑战,成为需要突破的互联网核心技术之一.在互联网可信性缺失造成的众多潜在危害中,借助伪造源地址发起的分布式拒绝服务攻击(distributed denial of service,简称 DDoS)[1,2]是当前互联网重要的安全威胁之一.DDoS 攻击通过发送海量伪造源地址的报文至目标主机,使其超过处理负载上限或网络负载上限致使服务崩溃,是一种频繁发生、影响最为严重的攻击手段[3].由于 DDoS 强大的破坏能力以及带来的经济损失,国际互联网标准化组织(Internet Engineering Task Force,简称 IETF)于 2015 年 6 月正式成立 DDoS 威胁协作(DDoS open threat signaling,简称 DOTS)工作组,专门研究减缓此类攻击的技术标准.然而,作为 DDoS 及众多攻击手段的依赖基础——“IP 源地址伪造”问题并未得到根本性解决.特别地,自治域间的 IP 源地址验证技术至今仍未形成任何国际标准.为了从互联网体系结构上解决安全可信问题,自治域间的源地址验证问题是必须应对和解决的关键挑战之一.

1 研究背景与现状

1.1 互联网安全现状及其与源地址验证技术的关系

由于互联网在设计之初假设用户可信,因此其在诞生之初就缺乏对网络安全的系统设计.随着互联网的快速普及,网络的发展速度也远超设计者的预期,互联网的使用人员从学术研究人员到如今庞大的异构的用户群体,设计之初假定的信任体系已不复存在,而保障网络安全已成为互联网持续发展的迫切需求.对于互联网安全现状及其与源地址验证技术的关系分析,主要涉及以下 3 个层面.

1.1.1 互联网体系结构

在 TCP/IP 的互联网体系结构中,IP 是互联网成功发展的核心环节[4].IP 协议层作为互联网的体系结构的“窄腰”[5],起到了承上启下的重要作用.也正因如此,IP 地址的安全性在很大程度上代表了整个互联网的安全根本[6].然而,互联网体系结构在设计之初假设所有网络成员都真实可信,并没有充分地考虑网络成员身份伪造带来的安全威胁,这使得构建在 IP 层之上的上层协议没有得到基础的安全服务保障,这使得伪造源地址攻击的能力超出了网络层范围,危害到其上层的协议,进一步扩大了“源 IP 地址伪造”带来的安全危害.

在 IP 协议的设计中,两个核心技术原则影响了相关防御技术与互联网体系结构的深度融合.

(1) 尽力而为的转发机制

考虑到网络通信的效率因素,高效地转发信息是互联网设计的重要目标,因此,互联网仅基于目的地址转发而不对源地址进行安全性验证.对于早期处理性能有限路由器而言,尽力而为地发送机制是必要而有效的.然而,当互联网用户规模不断扩大时,信任关系逐渐缺失,攻击者开始利用这样的网络结构,使路由器协助攻击者将攻击流量传出而不用担心其伪造源地址被发现.

(2) IP 语义重载

IP 地址承载着两个关键的信息:位置信息与身份信息.位置信息代表数据转发中对目标寻址及响应的标识,而身份信息代表通信用户的身份本体.在安全可信的互联网环境中,以位置信息作为核心标识的同时表征用户身份并不会产生任何问题,但伪造报文源地址却使得攻击者能在仿冒位置标识的同时隐藏自己的真实身份,直接造成了网络空间中大量犯罪行为难以被溯源的被动局面.

1.1.2 互联网 IP 地址管理与授权

IP 地址作为体系结构中的关键要素,作为通信建立的重要标识,其使用权限应该予以严格控制.IP 地址是由互联网号码分配局(Internet assigned numbers authority,简称 IANA)统一协调再经层层划分后才为用户所使用,经授权的 IP 地址需要通过网络设备的专业配置才能够被路由和访问.然而,地址的精确化层级划分及复杂的地址配置仅仅能够保证其作为目的 IP 的防伪能力,但对于攻击行为而言,采用非真实的源 IP 并未影响流量的传送,地址的授权并未对其作为“源”的使用而施加应有的限制.需要强调的是:由于对目的 IP 的伪造使得报文不能被传送至合法的目的地,这对于任何情况下的通信而言都是不具备任何意义的.因此,对于 IP 地址的伪造往往只针对源地址.

由于 IP 地址可在未经授权的环境之下使用,互联网将面临路由寻址与源地址两大重要的域间网络安全隐患.路由与寻址的安全隐患特指前缀劫持.在以边界网关协议(border gateway protocol,简称 BGP)[7]作为事实标准的域间路由系统中,自治域通过宣告一段不属于自己的地址前缀[8],使得访问该前缀的流量被劫持至这个非法的自治域内[9].源地址安全隐患是指域间源地址伪造.由于任何自治域所持有的地址可被其他自治域内的用户作为源地址使用,这使得流量的目的节点不能通过源 IP 地址来确定真实的通信对端身份,需要上层协议辅助才能确保通信可靠性.由于上述两种安全隐患的存在,使得互联网面临着严峻的安全挑战.

1.1.3 分散自治的网络运行体系

对于特定管理域的网络而言,由于管理者对域内路由系统有着完整的控制权限,其能够及时且妥善地处理网络中出现的各种突发状况;但对于分布式的互联网而言,各个自治域作为独立的经济实体或政治实体,任何人与任何管理域都不具备对整个网络的管理能力,而且各自治域/管理域之间由于缺乏协作,没有有效的手段对其他自治域/管理域拥有的地址的合法性进行判定.因此,网络环境的稳定性依靠于网络参与者对标准的执行能力,规范详尽的网络标准能够使参与其中的各个利益实体在未能完整控制世界网络的环境之下依然实现互联互通.然而,也正是这种去中心化的分布式结构,使得互联网中的自治域在遵循基础的网络标准之外显得高度自由,由体系结构引发的安全性问题也表现出高度不可控制的状态.

1.2 域间源地址伪造安全威胁分析

1.2.1 源地址伪造行为动机

源地址伪造产生的直接后果是增加被攻击者的防御难度.由于 IP 分组源地址能够被轻易篡改,构建在网络边缘的防火墙不再能根据 IP 地址进行安全性防护配置,在受害目标不对入域报文进行深度检测和分析的前提下,正常请求与攻击流量将难以区分,致使其在遭遇攻击时难以找到及时、有效的应对手段.然而,增加受害者的防御难度仅是伪造源地址的额外价值,而非主要动机.攻击者选择源地址伪造的原因主要可归结为以下两项.

(1) 隐匿攻击者的位置和身份[10]

现实社会行凶凶手通过伪造不在场证明,从而逃之夭夭,而网络黑客同样会尽其所能地在攻击发起时避免身份暴露而带来法律起诉.伪造源 IP 地址则成为网络攻击者隐匿身份的关键所在.由于 IP 语义重载的特性,攻击者在伪造 IP 源地址时能够同时隐藏位置信息与身份信息,却不会对攻击报文的路由传递产生任何阻碍,而特别对于在分布式的域间环境下,由于各自治域对外域报文不具有管理或控制的能力,在未得到外域配合的情况下,将难以对其源 IP 地址实施真伪判别.

(2) 放大攻击效果

网络中存在大量具备如下性质的网络协议:响应报文的长度是请求报文长度的数倍.即使某些协议不直接具备这个特性,也可以被攻击者间接利用,返回其所准备好的长数据报文.攻击者利用源地址可伪造性质的同

时,将源地址设置为受害者的主机地址,对部分公众服务发送相关的协议请求报文,服务端在收到请求后根据协议规范发送了一段比请求报文扩大几十至几百倍的响应报文至受害者主机,从而放大了攻击效果.特别是在域间环境下,若攻击者通过外域的反射而将攻击流量引至域外的目标域内,由于攻击节点和反射节点均不在受害域的控制范围之内,对于受害域而言,不仅攻击强度被放大,更为严重的是,其无法在反射之前拦截攻击流量,缺乏有效的遏制手段.

1.2.2 域间源地址伪造安全攻击现状

根据美国全球商务网络安全控制解决方案和服务提供机构 Arbor Network 发布的第 12 期《世界基础设施安全报告》[11],DDoS 攻击的最高峰值记录从 2010 年的 100Gbps 增长至 2016 年的 800Gbps,破坏性呈指数性提升,不断冲击着新的世界纪录.为了帮助全世界的安全机构及研究机构了解 DDoS 的攻击情况,Arbor Network 联合 Google idea 发布了如图 1 所示的 DDoS 可视化界面——数字攻击地图[12].数字攻击地图以国家为可视化界面单位,详细呈现了自 2015 年以来的每日规模前 2%的 DDoS 攻击信息,并揭示了国家间 DDoS 攻击的频繁性与严重程度.互联网的组成以自治域为基本运行单元,一般而言,每个国家具有一个至多个自治域.因此,频繁的、跨越不同国度的 DDoS 威胁表征着跨越自治域的伪造源地址攻击已日趋严重.

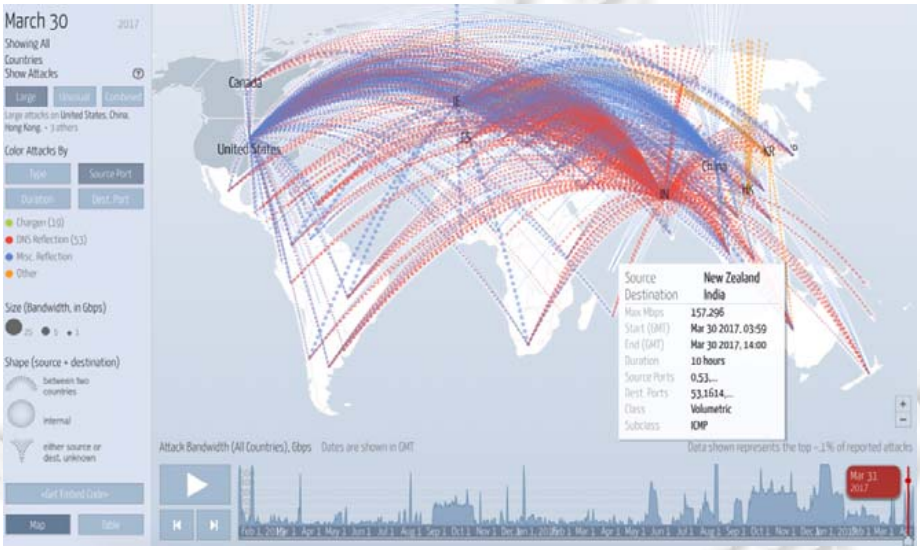


Fig.1 Visualization of top daily DDoS attacks worldwide

图 1 DDoS 攻击可视化页面

尽管 DDoS 可采用真实源地址进行攻击,但基于伪造源地址的 DDoS 威胁仍然占据主要部分.研究表明[13]:基于反射放大的 DDoS 近年来持续增长,利用 SSDP[14]、NTP[15]、DNS[16]和 CHARGEN[17]协议发起的反射式攻击成为 DDoS 攻击所依赖的主要载体,占据了近 50%的攻击流量.在所有反射式 DDoS 攻击中,最活跃的莫过于基于 NTP 的 DDoS 攻击和基于 DNS 的 DDoS 攻击,截止 2017 年 1 月,所检测到的单次最高攻击峰值已可分别达到 498Gbps 和 480Gbps,是大规模 DDoS 攻击的重要组成部分[11].考虑到流量通过反射形成的流量放大将直接增加攻击的破坏性,域间源地址伪造将持续成为域间 DDoS 攻击的重要依赖手段.图 1 选取了 2017 年 3 月 30 日的攻击界面,从攻击类型的区分对比中可以看出,反射式攻击仍是 DDoS 最主要的攻击手段.

2 实际部署与相关标准化研究近况

目前,源地址验证技术中唯一被标准化的且存在实际部署的技术是 IEF(ingress/egress filtering)[18,19].IEF 作为此类方法的初始实例,提供了最为精简的部署效能和最少的开销代价.IEF 通过在各个自治域的边界路由器

执行本地过滤检查机制:由于自治域内部可以明晰地掌握本自治域所持有的地址前缀,因此过滤出域流量中携带的伪造源地址报文相对容易.同理,亦可过滤由外域发文本域的、携带本域源地址的伪造报文.不难推断:若IEF全局部署,域间源地址伪造将被彻底消除.也正因如此,IETF接连将IEF的两项标准化文档评选为“当前最佳实践”标准.

然而,简洁、高效且无需自治域协作的IEF并没有在全球迅速推广.从自治域部署层面来看,运营商的核心工作是保障合法用户的互联互通,而对于合法用户进行严格的基于IEF的源地址验证不能提升用户体验,仅能约束域内用户不向外发送伪造报文而使整个互联网受益,却难以从互联网中得到自我保护.因此,从绝大多数自治域的部署状况来看,源地址验证仅仅是被看作为锦上添花的附加价值,而保障用户服务体验的互联互通仍是其对于客户服务的第一要义.缺乏部署激励反馈,使得自治域没有足够动力去执行IEF防御技术.

2.1 最佳实践部署近况

由于源地址验证的重要性,IETF早在2004年就完成了对IEF的标准化,其标准化成果也迅速被欧洲IP网络论坛RIPE、互联网社区Internet Society以及国际电信联盟ITU等标准化组织所采纳.其中,RIPE于2006年成立了反源地址伪造特别任务组[20],Internet Society的“部署360计划”也设置了反源地址伪造专区[21],并撰写了相关白皮书[22]以协助IEF的普及.然而,如上文所述,由于缺乏部署激励的原因,IEF的部署率在近年来反而逐渐降低[23],就连已部署的自治域也陆续关闭了防御功能[24],而RIPE的反源地址伪造特别任务组仅在成立18个月之后即迅速关闭.为了探测IEF的实际部署情况,CAIDA提出了Spoofer计划[25],请求志愿者主动参与IEF的部署探测,德国的网络实验室Internet Network Architectures也联合了700个互联网交换节点进行IEF的部署探测[26].由于DDoS攻击日趋严重,RIPE于2015年重新召开BoF会议,探讨源地址验证技术工作组成立的可行性[27],Internet Society也建立了路由安全联盟MANRS[28],号召大型自治域主动签约联盟以参与到IEF的部署中来.尽管如此,源地址伪造的安全态势并没有因为IEF的标准化得到缓解,反而日趋严重.

2.2 源地址验证体系结构

由于IEF部署的困难性,国际标准化组织IETF对源地址验证进行了系统性梳理,并于2008年提出了源地址验证体系结构(source address validation architecture,简称SAVA)[29].SAVA是一项由中国主导的国际化标准,其明确了源地址验证的研究框架,对源地址验证的发展具有重要意义.SAVA将源地址安全防御划分为3个层次:接入子网、自治域内、自治域间,各个层次呈现互不重叠的松耦合防御形式,共同建立成为完整的源地址验证体系.

(1) 接入子网源地址验证

接入子网位于3层防御体系结构中的最底层,其通过报文监听建立规则并定标,将伪造报文在其转发过程中的第1跳交换机处予以丢弃,能够实现主机粒度的源地址验证,也是3层防御体系中唯一一个形成标准化工作组的防御层面.但是,接入子网防御技术仅能够保证接入子网用户无法发起源地址伪造,并不能确保其收到的外域报文不被伪造.缺乏对外域攻击的防御、具备较大的防御代价,是本层防御结构的主要特点.

(2) 自治域内源地址验证

自治域内源地址验证位于3层防御体系的中间层,其主要用于过滤域内用户发起的伪造报文,具备适中的部署代价,与接入子网层相互补充共同构建出完整的域内防御体系.由于域内拓扑相比域外更为稳定,自治域通过获取自治域内的地址分配及路由策略建立准确的过滤规则并非难事,但其仍然只能约束域内用户行为,无法对外域攻击建立防御基础,对部署者的激励仍旧欠缺.

(3) 自治域间源地址验证

自治域间作为3层防御体系中的最上层,与前两层的防御作用存在明显差异.自治域间的源地址验证通过不同自治域的相互协作传递过滤特征规则,达到过滤域外源地址伪造报文的效果,构成防御体系中的最后一环.作为唯一能够过滤外域伪造报文的防御环节,自治域间源地址验证具备最粗的过滤粒度,部署代价更小、可扩展性更好,在分布式的互联网结构中更具部署激励和现实意义.

由于 SAVA 对防御模型的层次化区分,其突出了自治域间源地址验证系统的重要战略地位,在源地址伪造的严峻背景下,建立 SAVA 防御体系的最后一环:自治域间源地址验证,不仅能够较大程度地提升部署节点的安全性,而且为从体系结构的角度解决互联网安全问题提供了重要的基础和手段.在 SAVA 体系结构的基础上,中国学者在 IETF 中推动并成立了源地址验证增强(source address validation improvement,简称 SAVI)工作组[30].SAVI 工作组针对接入网技术,实现主机粒度的源地址安全保证.SAVI 通过制定交换机监听策略标准获取主机授权的合法 IP[31],确保主机发送的后续数据报文采用真实 IP 源地址,丢弃伪造源的数据报文.截止 2016 年底,SAVI 工作组任务已趋近完成[32].对于 SAVA 体系结构而言,最重要的是实现域间层面的源地址验证.对比于域内流量,自治域间具备更大的路由地址空间和巨大的网络流量,任何过滤策略上的复杂性都会造成庞大的开销并极大地降低了域间路由的效率.因此,设计轻量且高效的域间源地址验证策略,是相关研究及标准化组织关注的研究重点.

3 域间源地址验证的意义

现有的互联网体系结构缺乏对 IP 源地址伪造行为的监测机制,这使得当攻击行为产生时,恶意流量难以得到有效的溯源.尽管对于基于 Smurf[33]的 DDoS 攻击可以禁止来自其他网络的广播报文实现安全防御;对于基于 TCP SYN Flooding 的 DDoS 攻击,可以通过修改 TCP 协议来减缓攻击强度[34];对于基于 DNS 反射的 DDoS 攻击,可以通过完善 DNS 交互流程减少攻击损失,但这些方法均不能从根本上解决问题.只要源地址仍能够伪造,就会有新的协议漏洞被攻击者发掘利用,而协议的设计者却要需要频繁地在各个协议之间进行斟酌和修复,难以甚至无法应对层出不穷的新型攻击手段.即使协议能够及时得以完善,在攻击与修补之间的“时差”仍将为社会带来巨大的经济损失,防御策略也将永久地处于被动的应急状态.除此之外,当设计者创建新的网络协议或网络应用时,还要考虑如何避免伪造请求的防御模式,这增加了系统复杂度,为网络的发展增加了潜在的阻碍.

根据 Akamai 安全防御部 2016 年第 4 季度安全季度报告[35]显示,由中国自治域 ASN4837(CNCGROUP)和 ASN4143(ChinaNet-Backbone)所源发的 DDoS 攻击长期占据着大量流量占比.然而,在缺乏有效的源地址验证措施部署之前,由于大部分网络服务均可被用作攻击的反射跳板,难以判定攻击实施的真实位置.为了树立稳定的国家安全形象、避免网络服务被利用而造成的影响,建立自治域间的源地址验证系统对于互联网而言具有重要的作用.通过总结归纳,实现域间源地址验证具有以下 3 个方面的意义.

3.1 对自治域运维者的意义

(1) 抵御域外流量攻击

相比于针对域内的安全防御措施,抵御域外的伪造源地址攻击无疑是自治域更加迫切的需求.由于自治域对域内网络有着较为全面的控制权,域内的相互攻击更容易得到及时的发现和控制,而来自外域的攻击在没有得到域间协作的基础上抵御难度极大.因此,建立有效的域间源地址验证技术,是自治域实现对域内保护的重要环节.

(2) 降低成为反射点的概率

由于反射攻击的存在,伪造源地址报文的目的地可能是攻击的反射点而非攻击目标.在该环境下,自治域内的公开服务均可能被攻击者利用并作为反射点进行汇聚和放大.部署域间源地址验证可以降低自治域被作为反射点的概率,避免被攻击者栽赃陷害,也能降低其他自治域因反射而被攻击的概率.

(3) 降低其他自治域被攻击的概率

由于域间流量往往流经多个自治域后才能到达目的地,倘若流量流经的自治域中存在域间源地址验证技术,则伪造源地址流量被过滤的概率将有所增加,因而目的自治域被攻击的概率将有所下降.通过部署域间源地址验证技术,部署自治域将降低其他自治域被攻击的概率,进而为其他自治域提供保护.

3.2 对网络安全的意义

构建完整的 SAVA 防御体系.尽管以 SAVI 工作组为代表的接入子网源地址验证以及以 IEF 为基础的出口

网关检测在很大程度上解决了源地址伪造问题,但若仅以此为基础来提升整个互联网的安全,则要求此类技术在世界范围内的全局部署.但现实情况并不理想.在不考虑通过接入子网部署源地址验证具备较高代价的基础上,即使在某个自治域内完成全局部署,也没有任何政策推进能够保证其他自治域也实现全局部署,这种依赖于对方部署的防御策略无法帮助自治域抵御外域攻击,存在一定的局限性.由于接入子网层面和自治域内层面都不具备防御外域攻击的能力,建立自治域间的防御策略是构建完整防御体系的重要环节.在源地址伪造报文遍布的域间流量下,针对跨域攻击的防御是不可或缺的.作为 SAVA 体系中最为重要的环节,建立自治域间源地址验证的防御技术是构成完整防御体系的核心与关键.

3.3 对互联网体系结构的意义

(1) 提升互联网的可管理性

防御域间伪造源地址攻击是互联网安全可信的重要保障:一方面,其为数据通信提供安全性保障,这使得非法的通信可被拒绝访问,可疑的通信可被溯源追查.此外,真实的报文源地址使得防火墙和其他访问控制设备可以对出入域报文基于真实 IP 地址进行精细化的管理和控制,提升了网络管理的灵活性,降低了管理的复杂性.

(2) 提升互联网的稳定性

由于互联网的分布式特性,在缺失域间防御策略的环境下,伪造源地址报文从某一自治域发往网络中的其他节点时,势必会对其造成破坏并使得整个网络稳定性失衡.构建出完整的域间防御体系,将使伪造报文仅仅停留在报文发起的自治域本身,攻击带来的影响不会向互联网中继续扩散,这使得分布式的网络架构具有更强的稳定性.

(3) 为基于 IPv6 的地址技术创新提供保证

IPv6 的巨大地址空间为体系结构层面的技术创新提供了平台,而基于 IPv6 地址空间的技术创新需要以真实源地址为基础.利用 IPv6 网络更新换代的历史时机,从现在起严格按照区域类型和业务类型甚至用户类型进行地址分配,可使用户身份信息与 IP 地址的耦合更加紧密,也为用户身份识别与信息溯源提供了重要基础[36].

4 域间源地址验证技术

本节对域间源地址验证技术进行了归类和整理,并首次从“基于加密、签名及标记信息”“基于域间路由信息”“基于 IP 分组转发经历跳数”和“基于自治域间商业互联关系”的角度出发,对典型的相关技术进行了详细的分析.需要强调的是:尽管仍有其他分类方案可用于源地址验证的归纳(如“基于端到端”以及“基于路径”的分类方案),但我们认为:按照本文的分类方案能够更加透彻地分析针对域间的源地址验证技术的原理及优势,也能更准确地归纳不同技术间的特征及所面临的挑战.此外,尽管学术研究中同样存在大量的攻击追溯方案试图震慑网络犯罪[37],但这类方案并未从根本层面解决源地址伪造的客观事实,也不具备对互联网体系结构的安全弥补能力.因此,本文对防御技术的介绍将限制在域间伪造源地址验证的范畴,而不试图涵盖源追溯技术.

4.1 基于加密、签名及标记信息

4.1.1 技术原理

针对基于加密、签名和标记信息的域间源地址验证技术而言,研究通常采用端到端特征验证的设计结构.这种结构并非均以自治域作为设计单元,但仍可对域间环境做出大量优化改进.其中,端到端特征验证以密钥协商最为常见.通信双方在事前协商可供彼此验证的校验标识,并将其加载在通信过程中的数据报文内以供接收方进行身份确认.若接收方验证通过,则判定通信对端真实而接收报文;否则,视其为伪造而丢弃报文.

4.1.2 典型技术实例

(1) SPM(spoofing prevention method)[38]

SPM 作为此类技术的典型代表,衍生出了大量改良方案.SPM 的核心思想在于建立安全联盟体系,任何自治域都可以自愿地加入这个安全联盟.处于安全联盟内部的自治域成员需要承担律己的基础责任,即:对于发往安全联盟成员内的数据报文进行伪造源地址过滤检测,并在此基础上对发送的合法源数据报文添加其与目的端

事先协商的特定标签 Tag(Source,Destination)供目的端进行真实性检验,以防止安全联盟内外的任何其他自治域伪造本域源地址向此通信对端尝试非法通信.SPM 的典型特征在于这种联盟系统的俱乐部经济学模型,“防御”功能作为俱乐部物品仅为俱乐部会员之间相互提供,而俱乐部以外的成员则不享有俱乐部中的“防御”服务.然而,对于发生在联盟外对内的反射式攻击,联盟成员则不具备区分能力,只能争取扩大联盟范围以降低受到联盟外反射攻击的概率.

(2) DISCS(distributed collaboration system)[39]

DISCS 在 SPM 的基础上完善了方案实施方法,并进一步提升了方案的执行效率.DISCS 通过在 BGP 消息中设置可选、可传递的路径属性,以辨识不同的子联盟,当自治域在接收到若干 BGP 报文后,可选择加入与之存在利益共识的联盟,并最终将整个互联网划分为多个并行的防御联盟,每个联盟内提供与 SPM 类似的防御保护,但联盟之间并不建立防御共识.DISCS 赋予防御技术的最大贡献在于,将防御功能分时空地按需调用执行.DISCS 将防御功能划分为 4 个防御函数:目的保护、密码学的目的保护、源保护以及密码学的源保护.当联盟成员仅在受到攻击之时,根据攻击类型,按需调用联盟成员所提供的防御函数,并在攻击停止后解除调用.按需调用的协作方式不仅使得防御过程中的高开销问题得以缓解,还会尽可能地降低误判发生率,使假阳性指标在可控范围内进一步趋于最低.而安全地组成各个联盟,是 DISCS 面临的最大难题,联盟建立的可靠性依赖于 BGP 的安全性,在 BGPsec 得到广泛部署之前,DISCS 的部署激励仍然无法保证.

(3) 其他技术实例

MIEF[40]的设计同时借鉴了 IEF 过滤方法以及 SPM 的联盟体系,在不构建密码体系的基础上组成安全联盟,降低了部署开销,但也降低了防御效能.SMA[41]在 SPM 的基础上进一步加强了控制层面的安全性保障,以同步的状态机来取代复杂频繁的密钥交换,提升了技术本身的抗攻击能力.Passport[42]在借鉴防御联盟体系的同时增加了路径的检验机制,使之具备路径验证和对端验证的双重特征.然而,Passport 不可避免地引入了两者的缺陷,其路由动态性将严重影响密码学校验的准确性,相比 SPM 而言,具有更高的假阳性[43].

4.1.3 技术特征分析

由于此类方法应用的安全性即采用加密技术的安全性,因此,增强加密系统的破解难度并降低密钥被破解后造成的损失程度,是采取此类方法时所需考虑的重点.综合分析此类源地址验证技术的原理及优劣,其主要技术难点在于设计安全、高效的标签协商方案,即,端到端特征协商方案,避免协商过程中的脆弱性而引发出相应的安全攻击.此外,密钥协商的复杂性使得此类方案在大规模部署时具有较大的维护开销,可扩展性受限,制约了其实用价值.

4.1.4 技术优缺点

基于加密、签名和标记信息的域间源地址验证技术的优势在于不受网络拓扑动态性影响,过滤性能仅与拟采用加密算法的验证特征相关,且不具备固有假阳性,极大地规避了自治域部署的运维风险.然而,由于通信双方的数据报文不可避免地需要携带验证所需的特征信息,这使得数据平面产生了额外的通信开销.并且,过多的对端校验开销使其方案本身也极易成为 DDoS 的攻击目标,因而造成网络拥塞甚至服务瘫痪;而伪造源地址报文的过滤通常仅在通信对端执行,且在网络传输的过程中仍消耗着网络带宽,并未避免网络带宽资源的消耗浪费.

4.2 基于域间路由信息

4.2.1 技术原理

基于路由信息的源地址验证技术,其绝大部分可以针对域间体系做出优化设计.此类方案的设计思想在于:攻击者仅能伪造数据报文的源地址信息而不能控制报文的转发路径,当伪造源地址的数据报文从非法的路由端口进入时,路由器可进行真伪性验证以过滤伪造报文.DPF(distributed packet filtering)[44]作为路由过滤技术的方案框架,描绘了以路由器为过滤核心的技术蓝图.DPF 通过对各个路由器的各转发端口建立合法源地址绑定列表,并对转发过程中接收到的绑定列表范围之外的源地址报文判伪并丢弃.

4.2.2 典型技术实例

(1) IDPF(inter-domain packet filtering)[45]

IDPF 是以 DPF 为过滤基础的方案中最具代表的一个技术实例.IDPF 通过学习 BGP Update 报文获取各段前缀的路由方式,通过假定每段前缀的抵达端口与转发端口一致,从而独立地通过监听 BGP 报文来建立过滤规则.IDPF 的最大优势在于:其免除了自治域间的相互协作,极大地提高了部署的可行性.然而,独立预测使得部署自治域不能获得真实完整的路由信息,且路由宣告路径并非一定表征着前缀可能到达的方向,因此存在固有的假阳性.此外,由 IDPF 方式建立的规则集存在较大的规则空间,这使其过滤粒度较粗,并不具备良好的过滤性能.

(2) SN(selection notice)[46]

为了能够准确地建立过滤规则,最直接的办法是将路由选择通告至目的前缀,从而使沿途的各个自治域都能够为其建立相对完美的过滤规则.SN 为 BGP 增加新的选路通知报文:当自治域接收到 BGP 路由更新时改变路由策略,均需要将新的选路策略通过 BGP 选路报文告知目的对端,而沿途所经各个自治域均可通过学习选路通知报文为其建立过滤规则.SN 做出的最大调整在于将选路策略作为基础信息共享给沿途所有自治域,这与域间 BGP 策略路由的设计目标存在差异,并未得到各个运营商的认可.另外,由于 SN 与 BGP 的紧密耦合使得域间路由震荡时刻影响着方案的稳定程度,其所造成的运维风险也将制约着此类方法的实际应用价值.

(3) 其他技术实例

uRPF[19]假设到任何特定目的地址的流量均会从相同的端口流入,即,假设流量具备对称性并以此为过滤基础.尽管这样的方法在靠近用户的网络侧具备较强的执行效率,但“此断彼通”的健壮性使得域间网络并不具备这样的特殊性质,也因此削减了其有效验证范围,实用价值较低.SAVE[47]协议通过构建新的独立交互协议,使各路由节点能够共享选路决定.然而,域间路由的动态特性使得 SAVE 方案将因此产生反复的震荡,产生较大的控制开销;尽管 SAVE 的后续演进方案 iSAVE[48]增加了对增量部署的支持问题,但实现机制仍较为复杂.BASE[49]将部署节点划分为逻辑邻居,通过 BGP 消息作为媒介实现非邻接节点的协作,相比独立预测验证规则的 IDPF 而言,具有更好的验证准确性,但却并未完全规避假阳性的发生.

4.2.3 技术特征分析

建立基于域间路由信息的过滤技术需要依赖两项基本因素以建立过滤规则.

(1) 获取自治域号对所持前缀的合法映射

受商业保密策略的影响,自治域通常将保密其所持的合法地址前缀,使得任何其他自治域都无法确切掌握每段地址前缀的真实归属,因此也就更难以为其建立有效的过滤规则表.然而,为了确保网络服务的互联互通,自治域不可避免地需要对其所持有的地址前缀进行通告以保证网络可达性,这使得自治域与其所持前缀之间存在基础的映射关系.然而,前缀劫持攻击的存在使得这样的信赖体系不再具备可靠性,而建立自治域号与 IP 地址的映射关系的互联网基础设施,将是网络安全的必要途径.

(2) 获取源端路由选择信息

综合分析此类源地址验证技术的特性及原理,其最大的难点在于如何获取源至目的的转发途径并动态地建立验证规则.BGP 作为域间路由协议的事实标准,其策略路由的本质使得各个自治域不对路由选择做出任何承诺或保证.相反地,路由选择作为相对机密的信息被各个自治域所隐藏,这也使得每个自治域难以获得权威的信息用以过滤伪造报文;而若为了能够获取足够详尽的路由信息,不可避免地需要修改已有协议,甚至构建新的协议,这对于以自治域为粒度的开放式互联网产生了较大的阻碍.

在能够确保获取生成过滤规则的两项必备要素的前提下,生成验证规则并不是难事.通常情况下,按照过滤的维度,可将验证规则分为二维过滤以及一维过滤.二维过滤方案下,需要同时考虑路由的源与目的信息以进行过滤匹配,因此具有较为完美的过滤效能,但考虑到自治域间庞大的路由实体,构建二维过滤所需的全局路由信息难度极大,加之自治域间庞大的地址空间,使得这一复杂度为$\theta(n^2)$的过滤方案难以具备切实的执行能力.而一维过滤仅以源地址作为路由器过滤标准,将复杂度降为$\theta(n)$的同时提供了接近于二维过滤的防御能力,具备更高的可行性.

4.2.4 技术优缺点

不同于基于加密、签名及标记信息的源地址验证技术,基于域间路由信息的源地址验证方法能够使伪造报文在传输途中被尽早过滤,从而保护了带宽资源的有效利用,其分布式的验证机制也要求验证规则必须根据路由变化而改变,因此具备较强的自适应性.然而,此类源地址验证技术通常需要广泛的部署才能够取得较佳的过滤性能,而过滤规则的建立受到路由动态性的影响,若其未能及时适应新的路由变化而更新过滤规则,将会产生较为明显的假阳性及假阴性.

4.3 基于IP分组转发经历跳数

基于 IP 分组转发经历跳数的验证技术特指跳数计数过滤(hop count filtering,简称 HCF)[50].HCF 不同于上述两类源地址验证技术,它巧妙地利用了报文 TTL(time-to-live)剩余跳数的可行性范围来确立对端实体的合法性.由于通信双方的数据报文具备较为统一的转发路径,因此也应具备相对稳定的路由跳数.通信接收端在接受报文前对报文已转发跳数进行计算,若对于特定的通信源地址而言,其报文跳数在合理的范围之内,则可相信其在很大程度上未被伪造.

HCF 的特征在于将验证执行的位置移至通信主机,并未针对域间而进行设计优化.而为了减小拓扑震荡时产生的误判,HCF 仅能保持较粗的过滤粒度,过滤能力相对有限.尽管 HCF 消除了密码学带来的庞大计算开销,但其并不能取代为其提供的更为严密的安全保障.另一方面,互联网同样不对 TTL 的伪造执行任何检查,使其验证技术在得到攻击者足够“重视”后可以被彻底绕过.因此,HCF 作为一种轻量级的过滤技术仅能作为辅助防护,并不能作为核心安全技术应用在过滤防护策略之中.

4.4 基于自治域间商业互联关系

4.4.1 技术原理

自治域与自治域之间目前存在着两种最为主要的商业关系:Provider-Customer 和 Peer-Peer.Provider 需要为其 Customer 提供接入互联网的保障,也正因如此,Customer 需要为其通往 Provider 的流量而付费;而当两个自治域在网络规模相当的情况下,可建立 Peer-Peer 关系,处于 Peer-Peer 关系的自治域可以相互传递网络流量而无需承担任何流量费用.尽管域间的网络流量是遵从 BGP 协议而产生的,但 BGP 协议的背后实质上却是自治域间的商业关系.自治域间的商业关系存在一种最为显著的商业特质:Valley-Free[51],即无低谷特性.Valley-Free 特性使得任何自治域都没有动力去为自身及其 Customer 以外的任何流量付费,这表征着当网络流量穿越某一自治域时,自治域将至少从流量的某一端受益,即,不提供任何无偿的穿越服务.正是因为这样的具备极强商业性质的域间特征,使得自治域不会将其所有的路由信息毫无保留地向外宣告,每个自治域只会对特定邻居宣告能够从中攫取收益的路由通告,这使得能够在自治域之间传递合法流量路径的可行性空间大幅度缩小.

正是因为受到自治域商业关系的启发,以域间互联关系作为过滤基础的防御方法开始在学术界提出.由于商业关系是域间路由流量流向的最终本质,以自治域商业关系为基础的过滤方案相比其他方案更加精炼和简要.由于其仅从商业关系出发构建过滤策略,使得方案的部署将不受任何因域间路由缺陷而产生的固有限制或束缚,两者相互独立亦相互配合,防伪过滤在先,寻址转发在后,共同构建出相互并列的、如图 2 所示的整套分布式域间协作系统.

Fig.2 Distributed inter-domain cooperation system

图 2 分布式域间协作系统

4.4.2 典型技术实例

据目前所知,纯粹以自治域间商业互联关系为基础建立的防御系统仅存在 Arbif[52]一种技术,此类验证技术有待于进一步细化和完善.Arbif 运行模式与域间路由协议 BGP 存在共同之处,它以自治域商业合作关系为基础,在相邻部署自治域内传递过滤规则.部署自治域在启动防御技术时,其过滤规则生成引擎在其邻居之间建立通信连接,生成初始过滤规则,并根据商业关系导出表选择性地将部分过滤规则传递给特定的部署邻居.部署邻居在接收到新的过滤规则后,判断是否需要更新自身过滤规则表,若更新发生,再决定是否选择性地将部分过滤规则继续传递给具备特定商业关系的部署邻居.在过滤规则更新传播中,规则将以自治域号的形式不断扩散,这要求部署自治域直接相邻,但 Arbif 却未能对增量部署策略提出好的建议,这给在现实中推广带来较大的阻碍.Arbif 作为一种域间源地址验证技术的解决思路,很多细节并未得到详细的设计考虑.但其首次将自治域间的商业关系作为域间源地址验证技术的依赖基础,具备充分的灵活性与可扩展性,符合互联网不断演进的特征需求,具有良好的研究前景.

4.4.3 技术特征分析

此类方案的难点在于如何获取完整的域间商业关系.在目前的商业协商环境下,互联关系仍然是自治域间的重要商业机密,在未得到完整的解决方案之前,任何自治域都不愿意将此商业机密与第三方共享,以免造成额外的损失.目前,已有若干检测方案[53]能够从 BGP Update 的报文监听中推算出各自治域之间的商业关系[54],准确率已可达 95%以上[55].然而,一方面,利用这些方案获取的商业关系未能保证 100%的正确性[56],仍使得过滤技术有少许假阳性存在;另一方面,由于商业关系是通过 BGP 获取的,使得过滤系统未能与路由系统完全分离,从而降低了防御方案的灵活性和扩展性.如何在最小代价范围内使自治域之间共享商业信息并以此建立防御基础,是此类方案的研究重点,这需要标准化、商业激励等综合因素的共同作用才能达成良好的新型互助模式.

4.4.4 技术优缺点

由于基于自治域商业关系的过滤方法采用分布式的验证机制,过滤规则将随商业关系变化而动态更新,具备良好的自适应能力.从本质上获取域间流量的合法途径使其规避了 BGP 存在的诸多问题,且能够使得报文在传输路径中被尽早地过滤,具备更为良好的可扩展性和部署能力.但在此体系环境下,防御技术仍需广泛部署才能取得良好的过滤效能,而构建完整的、与路由体系相互补充的防御系统无疑需要更加完整的设计方案和部署激励策略,同时也需要国际标准化组织的支持才能取得长足的发展.

4.5 源地址验证技术演进趋势

通过对各源地址验证技术的原理进行细致分析,图 3 展示了各项方案的技术演进脉络.

在基于域间路由信息的源地址验证技术中,uRPF、SAVE、IDPF、SN 均是以 DPF 思路为基础的源地址验证方案.此外,由 IDPF 引申出的 IDPF Preference[57]借鉴了自治域商业关系的设计思想,利用自治域间商业关系对 IDPF 的可行解空间进行降解,提升了 IDPF 的验证效力.CatchIt[58]通过结合 SN 方案与 BASE 方案的技术特点,利用 TCP 连接在部署节点间实现路由选择通告.尽管 CatchIt 能够实现一定的部署激励,但未部署的自治域同样能够收到额外的防御保护,缺乏长期的部署指导方针.IPVF[59]在 SN 模型的基础上参考了 HCF 的跳数特性的限制,这使得过滤规则不但基于报文的来源方向,同时也基于域间路由跳数,这进一步地缩小了过滤规则的空间,提升了过滤的效能,但并不能因此而改变自治域间共享商业信息的疲软态度.

除此之外,IPsec[60]以及 IATH[61]是基于加密类的方案中最为成熟的安全解决方案.IPsec 作为主机粒度的加密协议,已被采纳为虚拟专用网 VPN 的标准之一,而 IATH 作为 IPsec 的隧道模式,能够适应自治域粒度的源地址验证,具备极强的安全性.然而,对于 IATH 而言,相同自治域的不同边界路由器必须拥有独立密钥,这使得秘钥维护规模从自治域个数规模扩大到边界路由器个数规模,可扩展性较差.

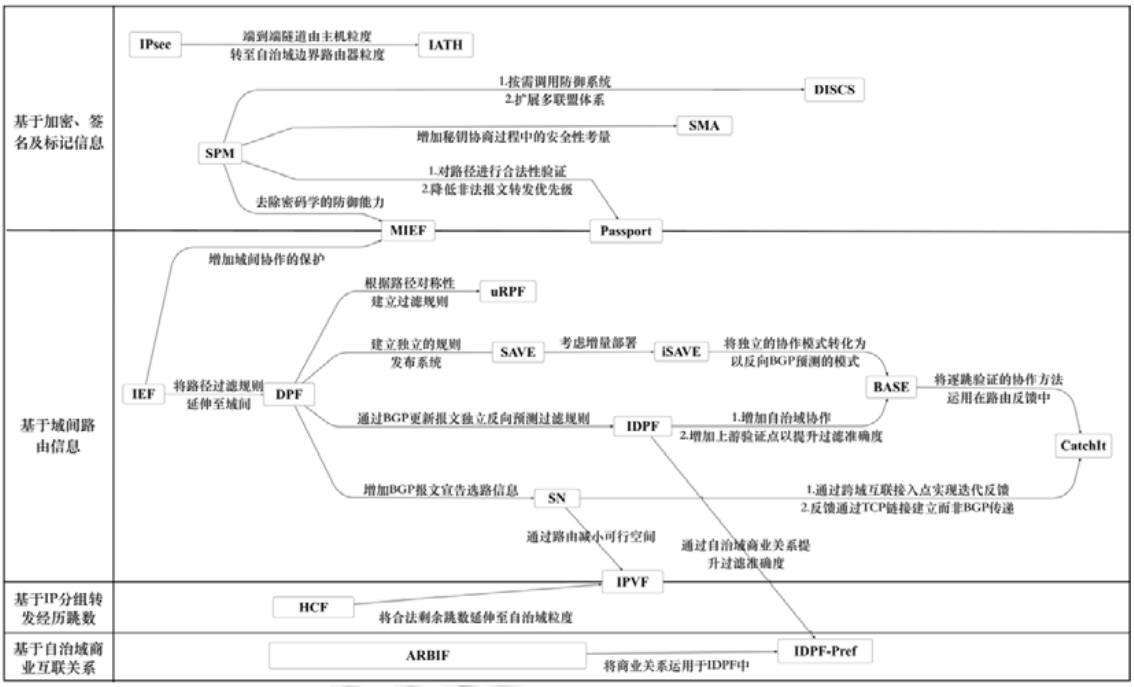


Fig.3 Choroid of evolution in inter-domain source address validation

图 3 域间源地址验证防御技术演进脉络

4.6 源地址验证技术特征归纳

综合分析各个技术的特征及性能,表 1 以文献[62]和文献[63]所提出的评价指标为基础,对域间源地址验证的技术特性进行了详细的归纳.

Table 1 Induction of source address validation characteristics

表 1 域间源地址验证技术特征比较

技术分类	技术	过滤位置	依赖技术	部署特征	制约因素	防御效力	实现开销
基于加密/签名/标记信息	SPM	源/目的端	加密技术	1. 仅部署者收益 2. 支持增量部署	可扩展性低	1. 假阳性低 2. 假阴性高	高
	SMA						
	DISCS						
	IPsec						
	IATH						
	Passport	传输路径					
基于域间路由信息	MIEF	源端	无				中
	IEF			部署激励低	部署激励低		低
	uRPF	传输路径	路径合法性	部署激励随部署率上升而逐渐降低	1. 未部署者受益明显 2. 受拓扑及路由动态性影响	1. 假阳性低 2. 假阴性高	未知
	DPF						中
	IDPF						
	SN						
	IPVF						
	SAVE						
	iSAVE						
	BASE						
基于域间互联关系	IDPF-Pref		商业关系				低
	ARBIF						
基于分组转发跳数	HCF	目的主机	报文跳数	仅部署者受益	防御可被彻底绕过	假阴/阳性高	

通过对比可知:基于加密、签名及标记信息的源地址验证技术往往具有较好的过滤性能,极少引入假阳性的风险,但复杂性和开销较高,规模可扩展性较低;而自治域间的商业关系作为互联网域间的本质特征,无论直接利用商业关系或是间接以域间路由信息为基础构建的防御技术均具有更好的灵活性和可扩展性.虽然此类方法暂时缺乏部署策略设计和有效的路由动态性适应机制,但其分布式的技术特性与域间系统更为契合,这更符合互联网发展的长期演进方向.

5 域间源地址验证技术面临的挑战

通过分析、概括各种方案的技术特征,域间源地址验证技术面临的挑战主要包括以下 4 个方面.

5.1 协议设计存在缺陷

在域间源地址验证防御方法的设计指导思想中,低风险、低开销以及高回报是评估协议的重要因素,然而,在已发表的学术成果中,尚未有任何一种方法能够三者兼顾.在源地址验证方案的设计中,存在两个重要的方案评估指标:假阴性与假阳性.

(1) 假阴性:是指对伪造报文的漏判率.假阴性代表过滤方案的过滤效能的高低,表征方案的辨伪能力;

(2) 假阳性:是指对合法报文的误判率.假阳性代表过滤方案的部署风险代价,表征方案的可靠性.

由于错误地过滤合法报文将极大地降低自治域的服务质量,一般情况下,自治域几乎不会考虑部署具有较高假阳性的过滤方案,但却能够容忍具有一定假阴性的验证方案.由于没有任何一种技术方案能够在各项评估指标中独揽大局,因此还没有一项技术得到广泛认可或成为国际技术标准.由于没有国际标准支持,网络设备厂商无法实现通用的域间过滤协议.而目前很多的过滤方法还需要修改主机协议栈,在没有标准支持的情况下,寻求厂商支持的可能性难度极大,即使部分部署,也很难产生预期的过滤效果.

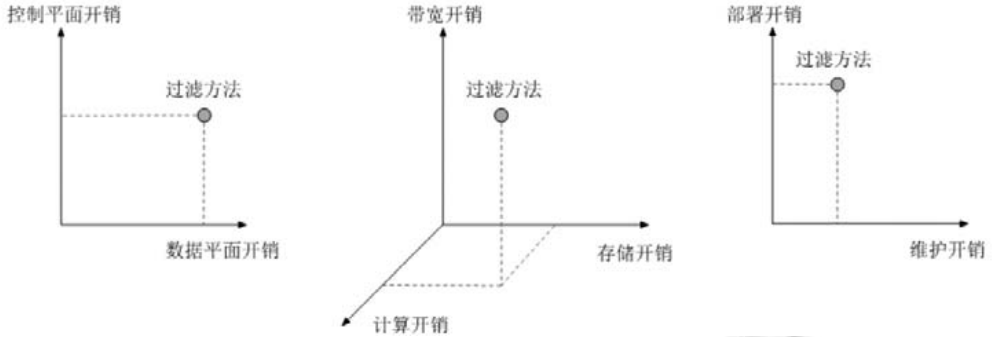
5.2 自治域间合作困难

由于单个自治域无法获取整个互联网的路由信息,因此也难以在缺乏有效信息协作的环境下构建误判率为 0 的过滤方案.为了建立更加完善的过滤技术,不可避免地需要自治域间的相互合作,通过传递过滤规则相关的必要信息,以求在降低假阳性的同时降低假阴性的比例.然而,由于商业与利益关系的阻隔,自治域间普适性的合作难以存在.其中,商业竞争与政治互斥是自治域实体之间的主要隔阂.商业竞争的自治域需要在互联网中抢占更多的用户及商业资源,而若要达成合作共识,则需交互大量的商业信息,而这其中的很大部分对于自治域而言仍属于商业机密.因此,要在相互竞争的自治域之间共享商业机密信息难度极大.而对于政治主张相斥的国家或宗教,其建立合作同盟关系将不低于两个商业竞争的自治域实体,甚至建立基本可靠的路由系统都不能得到切实保障.

5.3 协议开销过重

在目前可行的方案中,绝大部分需要增加极大的运维开销,部分方案带来的开销甚至远大于其服务性能得到的提升;而对于部分具有固有假阳性(高误判率)或过滤能力不佳(高漏判率)的技术方案,还会影响到已有的服务质量.因此,对于任何运营商,部署这样一套源地址验证方案都将面临巨大的开销代价.一般会按照以下 3 种分类方法进行分类:根据处理平面分类、根据开销性质分类以及根据开销类型分类.图 4 对开销代价多维空间进行拆解,并从各个维度独立展示了方案部署的开销空间.

从处理平面的角度分析,基于加密、签名和标记信息的源地址验证方案相较于基于域间路由信息方案而言,其数据平面和控制平面的开销均较高;从开销类型的角度分类,前者相较于后者具备更多的带宽开销和计算开销;从开销性质的角度分类,两者均存在不同程度的部署开销和维护开销.



(a) 根据处理平面分类 (b) 根据开销类型分类 (c) 根据开销性质分类

Fig.4 Multidimensional overhead space

图 4 多维开销空间

5.4 缺乏部署激励

对于大多数域间源地址过滤方案而言,在防御效能评价之前往往都对部署率有着过于乐观的评估,甚至存在部分方案需在全局部署的环境下才能取得预期的过滤效能的现象,但这在真实的互联网世界中是不具备实际执行力的.此外,部分验证方案对单一自治域在特定部署率环境下缺乏部署激励,即:从新增的部署节点角度出发,其部署后带来的过滤效能提升将随着部署率的增大而逐渐下降,这使得越晚部署的自治域部署激励越来越低,缺乏良性的激励推动方案的持续部署,影响其实际执行效能.另一方面,某些方案的过滤策略使得一些未部署节点能够间接地得到过滤保护,甚至在未部署的情况下得到不弱于部署节点的过滤效能,基于自治域作为商业实体的行为特征,这样的域间源地址验证方案推广将面临更大的阻力,“不劳而获”使得更多的自治域处于按兵不动、坐享其成的“被动”局面.

综上所述,域间源地址验证未能得到实际部署的原因可归结为效用与利益失衡.互联网服务提供商的投资都希望得到与之相比更多的回报,但目前的验证技术未能均衡地应对上述各类挑战.其中,基于加密、签名和标记信息的源地址验证方案开销过重,而基于域间路由信息的方案假阳性过大而运维风险过高,这使得域间源地址验证的挑战正逐渐转向于方案的可部署性问题.尽管大部分验证方法主要关心互联网安全所涉及的集体利益问题,并在一定部署规模的基础上具备较好的整体防御效力,但方法设计中极少涉及对各个自治域的部署激励,忽略了部署者的局部利益.自治域在缺乏利益驱动的背景下,部署代价难以转化为经济效益,阻碍了防御方案的部署推进.因此,建立以部署者利益出发的可部署性评价模型,已逐渐成为域间源地址验证的重要设计指标[64,65].

6 域间源地址验证技术发展展望

6.1 域间源地址验证未来研究方向

通过梳理各项源地址验证技术的发展脉络,结合互联网发展的指导思想,域间源地址验证技术应当以可部署性或部署演进为主要研究方向.未来,域间源地址验证系统的演进思路可借鉴 IPv4 向 IPv6 的过渡模式.初始阶段,源地址验证技术零星地在部分自治域之间开始部署,形成“海洋中的孤岛”;紧接着,部署范围开始不断扩展,部署的自治域不断增多,并逐渐成为“海洋”,而未部署的自治域变为孤岛;最终,所有部署方案实现全局部署,完成整个演进过程.不难发现:这样的演进趋势需要增量部署的技术策略以及标准化推进共同保驾护航,其中任何一种因素的缺失,都将带来方案推进的重要阻碍.此外,相互协作的商业互联关系,则将成为其演进延续的重要手段.

在此设想下,我们认为,域间源地址验证技术将按照图 5 所示的演进趋势以实现整个互联网的全局部署.在图 5 所表征的简略拓扑示意图中,自治域以单个路由节点的形式表示,其中,彩色和灰色分别表示已部署和未部

署源地址验证技术的自治域团体,而未来源地址验证技术的发展将从两个方面持续演进:已部署团体的不断扩张和部署团体之间的相互融合.当新增部署节点邻接某一已部署团体(以相同颜色表示)时,将扩张成为原团体的新组成部分,并相互协作以配置统一的防御策略;当部署节点不断增加而使两个原非邻接的部署团体(以不同颜色表示)直接相邻时,两者将同样合并成为一个新团体并重新更新统一的源地址验证策略,最终逐渐形成如水滴融合般的汇聚过程.

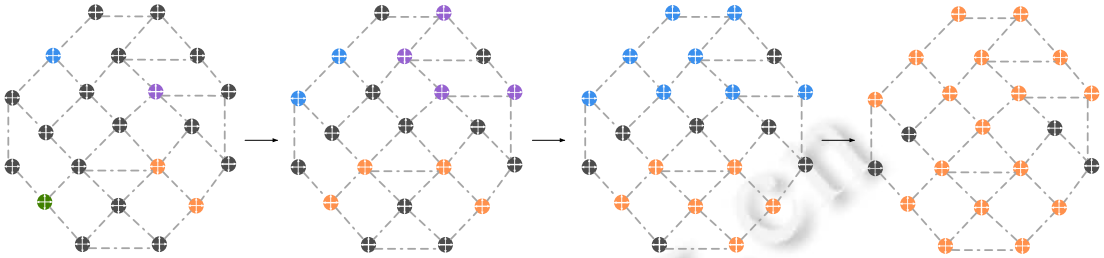


Fig.5 Blueprint of the evolution in validation techniques

图 5 验证技术部署演进图

在图论的形式化定义描述下,整个互联网可抽象成一个无向图 $G(V,E)$,其中,节点 V 代表一个完整自治域的形式抽象,而边 E 代表两个自治域之间形成的一类商业关系.定义某个特定时刻,源地址验证技术的复杂度为 θ,且图 $G(V,E)$的若干导出子图 $H_i(V_i,E_i)$,$i=1,2,3,\ldots,k$ 满足下述两个条件.

- H_i 之间相互独立,即 $H_m \cap H_n=\varnothing, \forall m,n\in i \wedge m\neq n$;
- H_i 是连通图,即 $\forall \alpha,\beta\in V(H_i), \exists path(\alpha,\beta)$.

于是有 $H_i(V_i,E_i)$为图 $G(V,E)$下的一个部署团体.在此基础上,定义新增部署节点 γ,并按照下述 3 类部署演进环境调整部署策略.

(1) 当 γ 的邻居节点均未存在于已部署团体时,将产生 $H_{k+1}(\{\alpha\},\varnothing)$的新部署团体;

(2) 当 γ 的任一邻居节点存在于 1 个已部署团体 $H_x(V_x,E_x)$时,H_x 扩张为 $H_x(V_x\cup\{\gamma\},E_x\cup E(\gamma\odot E_x))$,其中,$E(\gamma\odot E_x)$定义为 γ 与 $H_x(V_x,E_x)$团体存在关联的边的集合;

(3) 当 γ 的邻居节点存在于 2 个或 2 个以上已部署团体 $H_x(V_x,E_x)$,$H_y(V_y,E_y)$时,不同的团体相互融合,成为一个新的部署团体 $H_z(V_z,E_z)=(V_x\cup V_y\cup\ldots\cup\{\gamma\},E_x\cup E_y\cup\ldots\cup E(\gamma\odot E_x\odot E_y\odot\ldots))$.

对于特定的部署团体 $H(V,E)$,由于团体内部协商统一的源地址验证策略,其复杂度为 $\theta_H(1)$;而对于整个拓扑 $G(V,E)$而言,不同的部署团体之间相互协商通信标签建立保护机制,因此,当在存在 k 个连通子图 H——即 k 个部署团体的环境下,其复杂度为 $\theta_G(k^2)$.尽管部署节点的平均开销与部署增量策略有着直接联系,难以绘制明确的开销曲线,但在假定域间源地址验证技术在网络节点中随机部署时,能够形成如图 6 所示的开销变化期望曲线.其中,部署率的临界值表征当任何一个自治域参与部署时都将产生旧团体的融合从而降低连通子图个数,并逐渐降低开销带来的复杂度.由于融合所触发的良性循环将激励剩余团体的持续融合,部署节点将形成统一的极大连通子图 $H(V,E)\subseteq G(V,E)$,从而完成整个互联网环境的全局部署.

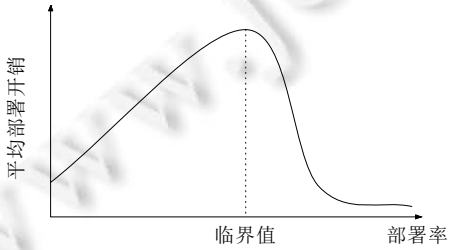


Fig.6 Expectation of the dynamic overhead

图 6 动态开销期望

由于商业互联关系从根本上决定着自治域间流量的传输方向,而相邻自治域节点可以已达成的商业关系为基础,建立易于聚集的、统一配置策略的部署团体,因此,邻接环境下的域间源地址验证技术可以 Arbif 为设计基础;而对非相邻部署团体的源地址验证策略而言,源地址验证系统可以 SPM 为技术原型来增加验证效力,同时参考 DISCS 方案中按需调用防御函数的设计思想.在融合过程中,当不相邻的部署团体因新自治域的参与而融合成新团体时,如何协调原“旧”团体的源地址验证策略,是其不断演进的重要挑战.与此同时,相关研究还需致力于部署节点对于融合的激励效力,即:在简化配置策略的同时使新团体的验证范围不低于融合前旧团体的直接加和,并以此为动力进一步吸引部署团体的持续融合.

6.2 对网络新技术的借鉴与结合

构建演进式的域间源地址验证系统,是域间源地址验证的发展方向.落实到技术本身,以自治域商业关系为基础的源地址验证技术仍具有较大的潜力,将成为未来研究的重点;而以软件定义网络(software-defined networking,简称 SDN)为基础的网络架构便于对网络进行动态定义和集中控制,若能成功迁移到域间互联网中,同样将具备重要的研究价值[66,67].此外,为了防止前缀劫持等域间路由攻击,IETF 安全域间路由(secure inter-domain routing,简称 SIDR)工作组建立了资源公钥基础设施(resource public key infrastructure,简称 RPKI)[68,69]以绑定自治域号与所持源地址空间[70].RPKI 的出现为实现域间源地址验证提供了切实可行的可信依赖;而对接 RPKI 的信任锚点,将成为未来域间源地址验证的重要手段.在此基础上,域间源地址验证在技术成熟后可逐步作为一项服务在网络运营商之间进行有偿提供[71],相关研究可充分利用商业利益对 BGPsec 部署推动的经验和方法[72],进一步促进域间源地址验证技术的部署.

6.3 域间源地址验证技术设计原则建议

通过对未来发展方向的分析,我们进一步提炼了未来域间源地址验证技术的设计原则建议.

(1) 增强方案规模可扩展性

正如前文所述,自治域间的跨域流量无疑是极其庞大的,源地址验证技术必须在设计之初保持轻量的技术特性,使得方案在部署量增加的同时,其多维的开销仍能够保持在较低的范围.由于域间源地址验证的终极目标是实现大范围部署,而任何复杂的技术部署在域间时都会遭遇极强的阻碍.因此,设计轻量、低开销和规模可扩展的协议机制,是域间源地址验证技术得以普及的根本.

(2) 提升协议功能可扩展性

域间源地址验证技术的功能可扩展性,决定了其对于互联网安全可持续发展的重要性.尽管 BGP 协议目前任然面对着诸多安全性技术问题,但其灵活性及功能可扩展性是其能够持续演进的根本所在.域间源地址验证技术的设计不应只立足当下,需要充分考虑协议的扩展能力和适应能力,使之能够容纳和应对互联网未来可能出现的各类安全挑战,并逐步发展成为域间安全协议的主干和事实标准.

(3) 简化协议交互信息

大部分防御技术之所以能够取得较好的仿真效果,是由于在防御协作中交互了大量网络基础信息,甚至商业机密.尽管为了构建防御体系,协作制度不可避免,但防御技术在设计之初仍需尽可能地为自治域本身考虑,减少交互信息中涵盖的商业机密,使得自治域能够在最大程度地维护商业机密的环境下达成合作共识,从而形成积极的意识形态以助力互联网的安全与发展.

(4) 将可部署性和激励策略作为协议的主要设计目标

目前,大部分源地址验证技术的研究都停留在仿真层面的性能分析,而缺乏实际部署测试与部署激励考量,这使得大量的实际问题被掩盖,甚至无法得到运营商的部署支持.此外,对于任何一项域间源地址验证的研究而言,提出一种有效的、能够促进自治域增量部署的解决方案,远比直接设计出一套完整的模型更有价值.例如,一些具备良好激励模型或经济模型的技术方案,尽管其不能完美地抑制攻击的发生,但却使得攻击的代价增加,进而使攻击者放弃继续侵略的念头,展现出与过滤技术效力相近的防御能力.

7 结束语

本文从互联网体系结构入手,分析了域间源地址验证的背景和标准化现状,通过将域间源地址验证技术划分为 4 个特征类别——基于加密、签名及标记信息,基于域间路由信息,基于 IP 分组转发经历跳数,基于自治域商业互联关系,本文对域间源地址验证技术的研究演进脉络进行了详细的梳理和归纳,深入分析了现有各种方案的技术特点.在此基础上,本文总结了域间源地址验证技术发展所面临的技术挑战,提出了域间源地址验证技术的设计准则和今后的发展方向,希望能够为后续相关研究工作的开展提供建议与参考.

检查网络中转发分组来源的真实性,本应成为网络体系结构支持的基本功能,然而,受众多因素的影响,这个问题至今仍未被解决,且持续地被用作实现网络攻击的重要手段.尽管学术界与工业界对此进行了广泛的研究与讨论,但目前仍未有适用于大规模部署的技术方案.为此,方案的可部署性正逐渐成为相关领域的研究热点.随着互联网新技术的不断出现,通过与网络新技术的融合,域间源地址验证的研究也将会不断完善.当新方案的效用与收益逐渐均衡、当部署的开销与风险逐渐可控,域间源地址验证技术才能够被网络运维者所认可与支持,互联网安全才能够被保障和加强.

致谢 感谢审稿专家对本文初稿提出的宝贵意见.

References:

[1] Handley M, Rescorla E. Internet denial-of-service considerations. RFC 4732, 2006. [doi: 10.17487/RFC4732]

[2] Mirkovic J, Reiher P. A taxonomy of DDoS attack and DDoS defense mechanisms. ACM SIGCOMM Computer Communication Review, 2004,34(2):39−53. [doi: 10.1145/997150.997156]

[3] Wang A, Mohaisen A, Chang W, Chen S. Delving into Internet DDoS attacks by botnets: Characterization and analysis. In: Proc. of the 45th Annual IEEE/IFIP Int'l Conf. on Dependable Systems and Networks (DSN). IEEE, 2015. 379−390.

[4] Wu J, Lin S, Wu K, Liu Y, Zhu M. Advance in evolvable new generation Internet architecture. Chinese Journal of Computers, 2012, 35(6):1094−1108 (in Chinese with English abstract). [doi: 10.3724/SP.J.1016.2012.01094]

[5] Wu J, Wu Q, Xu K. Research and exploration of next-generation Internet architecture. Chinese Journal of Computers, 2008,31(9): 1536−1548 (in Chinese with English abstract). [doi: 10.3321/j.issn:0254-4164.2008.09.007]

[6] Xu K, Zhu L, Zhu M. Architecture and key technologies of internet address security. Ruan Jian Xue Bao/Journal of Software, 2014, 25(1):78−97 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4509.htm [doi: 10.13328/j.cnki.jos.004509]

[7] Yakov R, Li T, Hares S. A border gateway protocol 4 (BGP-4). RFC 4271, 2005.

[8] Li S, Zhuge JW, Li X. Study on BGP security. Ruan Jian Xue Bao/Journal of Software, 2013,24(1):121−138 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/4346.htm [doi: 10.3724/SP.J.1001.2013.04346]

[9] Wang N, Du X, Wang WJ, Liu AD. A survey of BGP security. Chinese Journal of Computers, 2016,39 (in Chinese with English abstract). http://www.cnki.net/kcms/detail/11.1826.TP.20160920.2102.004.html [doi: 10.11897/SP.J.1016.2017.01626]

[10] Beverly R, Berger A, Hyun Y. Understanding the efficacy of deployed internet source address validation filtering. In: Proc. of the 9th ACM SIGCOMM Conf. on Internet Measurement Conf. ACM Press, 2009. 356−369. [doi: 10.1145/1644893.1644936]

[11] Anstee D, Bowen P, Chui CF, Sockrider G. Arbor Networks' 12th Annual Worldwide Infrastructure Security Report. 2017. https://www.arbornetworks.com/insight-into-the-global-threat-landscape

[12] Digital attack map: Top daily DDoS attacks worldwide. http://www.digitalattackmap.com/

[13] Mansfield-Devine S. The growth and evolution of DDoS. Network Security, 2015,2015(10):13−20. [doi: 10.1016/S1353-4858(15) 30092-1]

[14] Arukonda S, Sinha S. The innocent perpetrators: Reflectors and reflection attacks. Advances in Computer Science, 2015,4(1): 94−98.

[15] Czyz J, Kallitsis M, Gharaibeh M, Papadopoulos C, Bailey M, Karir M. Taming the 800 pound gorilla: The rise and decline of NTP DDoS attacks. In: Proc. of the 2014 Conf. on Internet Measurement Conf. ACM Press, 2014. 435−448. [doi: 10.1145/2663716. 2663717]

[16] Rozekrans T, Mekking M, de Koning J. Defending against DNS reflection amplification attacks. University of Amsterdam System & Network Engineering RP1, 2013. https://homepages.staff.os3.nl/~delaat/rp//2012-2013/p29/report.pdf

[17] Gillman D, Lin Y, Maggs B, Sitaraman RK. Protecting websites from attack with secure delivery networks. Computer, 2015,48(4): 26−34. [doi: 10.1109/MC.2015.116]

[18] Ferguson P, Senie D. Network ingress filtering: Defeating denial of service attacks which employ IP source address spoofing. RFC 2827, 2000.

[19] Baker F, Savola P. Ingress filtering for multihomed networks. RFC 3704, 2004.

[20] RIPE. IP anti-spoofing task force. https://www.ripe.net/participate/ripe/tf/anti-spoofing

[21] Internet Society. Anti-Spoofing. https://www.internetsociety.org/deploy360/anti-spoofing/

[22] Internet Society. Addressing the challenge of IP spoofing. http://www.internetsociety.org/doc/addressing-challenge-ip-spoofing

[23] Beverly R, Berger A, Hyun Y. Understanding the efficacy of deployed internet source address validation filtering. In: Proc. of the 9th ACM SIGCOMM Conf. on Internet Measurement Conf. ACM Press, 2009. 356−369. [doi: 10.1145/1644893.1644936]

[24] Internet Society. Initial longitudinal analysis of IP source spoofing capability on the Internet. https://www.internetsociety.org/doc/initial-longitudinal-analysis-ip-source-spoofing-capability-internet

[25] Caida spoofer project. https://www.caida.org/projects/spoofer/

[26] Franziska L, Florian S, Philipp R, Anja F. Illegitimate source IP addresses atinternet exchange points. https://ripe73.ripe.net/wp-content/uploads/presentations/12-Illegitimate_ips_at_IXPs_ripe73_franziska_lichtblau.pdf

[27] Andrei R. How do we address the problem of IP spoofing? And is it a problem worth solving? https://ripe71.ripe.net/programme/meeting-plan/bof/#tue1

[28] Mutually agreed norms for routing security (MANRS). http://www.routingmanifesto.org/

[29] Wu J, Bi J, Li X. A source address validation architecture (SAVA) testbed and deployment experience. RFC 5210, 2008.

[30] Nordmark E, Bagnulo M, Levy-Abegnoli E. FCFS SAVI: First-Come, first-served source address validation improvement for locally assigned IPv6 addresses. RFC 6620, 2012.

[31] Baker F. Source address validation improvement (SAVI) solution for DHCP. RFC 7513, 2015.

[32] Wu J, Bi J, Bagnulo M, Baker F, Vogt C. Source address validation improvement (SAVI) framework. RFC 7039, 2013.

[33] Kumar S. Smurf-Based distributed denial of service (DDoS) attack amplification in Internet. In: Proc. of the 2nd Int'l Conf. on Internet Monitoring and Protection (ICIMP 2007). IEEE, 2007. 25−25. [doi: 10.1109/ICIMP.2007.42]

[34] Eddy W. TCP SYN flooding attacks and common mitigations. RFC 4987, 2007.

[35] Akamai's state of the Internet report. Q4. 2016. https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/q4-2016-state-of-the-internet-connectivity-report.pdf

[36] Liu Y, Ren G, Wu J, Zhang SL, He L, Jia YH. Building an IPv6 address generation and traceback system with NIDTGA in address driven network. Science China (Information Sciences), 2015,58(12):1−14. [doi: 10.1007/s11432-015-5461-0]

[37] Yao G, Bi J, Vasilakos AV. Passive IP traceback: Disclosing the locations of IP spoofers from path backscatter. IEEE Trans. on Information Forensics and Security, 2015,10(3):471−484. [doi: 10.1109/TIFS.2014.2381873]

[38] Bremler-Barr A, Levy H. Spoofing prevention method. In: Proc. of the 24th Annual IEEE Int'l Conf. on Computer Communications (INFOCOM). 2005. 536−547. [doi: 10.1109/INFCOM.2005.1497921]

[39] Liu B, Bi J. DISCS: A distributed collaboration system for inter-AS spoofing defense. In: Proc. of the 44th Int'l Conf. on Parallel Processing (ICPP). IEEE, 2015. 160−169. [doi: 10.1109/ICPP.2015.25]

[40] Liu BY. Design on the deployability evaluation model of Internet Inter domain source address validation [Ph.D. Thesis]. Beijing: Tsinghua University, 2014 (in Chinese with English abstract).

[41] Shen Y, Bi J, Wu J, Liu Q. A two-level source address spoofing prevention based on automatic signature and verification mechanism. In: Proc. of the IEEE Symp. on Computers and Communications (ISCC 2008). IEEE, 2008. 392−397. [doi: 10.1109/ISCC.2008.4625684]

[42] Liu X, Li A, Yang X. Passport: Secure and adoptable source authentication. Networked Systems Design and Implementation (NSDI), 2008,8:365−378.

[43] Liu X, Yang X, Lu Y. To filter or to authorize: Network-Layer DoS defense against multimillion-node botnets. ACM SIGCOMM Computer Communication Review, 2008,38(4):195−206. [doi: 10.1145/1402946.1402981]

[44] 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. 15−26. [doi: 10.1145/383059.383061]

[45] Duan Z, Yuan X, Chandrashekar J. Controlling IP spoofing through inter-domain packet filters. IEEE Trans. on Dependable and Secure Computing, 2008,5(1):22−36. [doi: 10.1109/TDSC.2007.70224]

[46] Wang LJ, Wu JP, Xu K. BGP extension to support inter-domain distributed packets filtering. Ruan Jian Xue Bao/Journal of Software, 2007,18(12):3048−3059 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/20071208.htm

[47] Li J, Mirkovic J, Ehrenkranz T, Wang MQ, Reiher P, Zhang LX. Learning the valid incoming direction of IP packets. Computer Networks, 2008,52(2):399−417. [doi: 10.1016/j.comnet.2007.09.024]

[48] Ehrenkranz T, Li J, McDaniel P. Realizing a source authentic Internet. In: Proc. of the Int'l Conf. on Security and Privacy in Communication Systems. Berlin, Heidelberg: Springer-Verlag, 2010. 217−234. [doi: 10.1007/978-3-642-16161-2_13]

[49] Lee H, Kwon M, Hasker G, Perrig A. BASE: An incrementally deployable mechanism for viable IP spoofing prevention. In: Proc. of the 2nd ACM Symp. on Information, Computer and Communications Security. ACM Press, 2007. 20–31. [doi: 10.1145/1229285.1229293]

[50] Wang H, Jin C, Shin KG. Defense against spoofed IP traffic using hop-count filtering. IEEE/ACM Trans. on Networking (TON), 2007,15(1):40−53. [doi: 10.1109/TNET.2006.890133]

[51] Gao L. On inferring autonomous system relationships in the Internet. IEEE/ACM Trans. on Networking (ToN), 2001,9(6):733−745. [doi: 10.1109/90.974527]

[52] Wu J, Ren G, Li X. IPv6 network inter domain source address validation technology research. Science Paper Online, 2007,2(10):715−719 (in Chinese with English abstract). [doi: 10.3969/j.issn.2095-2783.2007.10.003]

[53] Fan QL, Yin H, Lin C, Dong JQ, Song W. Inference algorithms of Internet autonomous systems business relationships. Chinese Journal of Computers, 2014,37(04):950−962 (in Chinese withEnglish abstract). [doi: 10.3724/SP.J.1016.2014.00950]

[54] Shavitt Y, Shir E, Weinsberg U. Near-Deterministic inference of AS relationships. In: Proc. of the 10th Int'l Conf. on Telecommunications 2009. IEEE, 2009. 191−198. [doi: 10.1109/INFCOMW.2009.5072167]

[55] Luckie M, Huffaker B, Dhamdhere A, Giotsas V, Claffy KC. AS relationships, customer cones, and validation. In: Proc. of the 2013 Conf. on Internet Measurement Conf. ACM Press, 2013. 243−256. [doi: 10.1145/2504730.2504735]

[56] Gregori E, Improta A, Lenzini L, Rossi L, Sani L. A novel methodology to address the Internet AS-level data incompleteness. IEEE/ACM Trans. on Networking (TON), 2015,23(4):1314−1327. [doi: 10.1109/TNET.2014.2323128]

[57] Yao G. Path-Based Internet source address validation studies [Ph.D. Thesis]. Beijing: Tsinghua University, 2011 (in Chinese with English abstract).

[58] Li J, Bi J, Wu J. Umbrella: A routing choice feedback based distributed inter-domain anti-spoofing solution. In: Proc. of the 20th IEEE Int'l Conf. on Network Protocols Network Protocols (ICNP). IEEE, 2012. 1–2. [doi: 10.1109/ICNP.2012.6459939]

[59] Zhang Z, Liu Y, Wu JP, Ren G, Bi J. An Inter-AS path vector filter: Towards elimination of false negatives. In: Proc. of the 21th IEEE Int'l Workshop on Local & Metropolitan Area Networks (LANMAN). IEEE, 2015. 1–2. [doi: 10.1109/LANMAN.2015.7114734]

[60] Kent S, Seo K. Security architecture for the Internet protocol. RFC 4301, 2005.

[61] Kent S. IP authentication header. RFC 4302, 2005.

[62] Lee S, Othman M, Udzir NI. IP spoofing defense: Current issues, trend and challenges. MASAUM Journal of Reviews and Surveys, 2009,1(1):110−116.

[63] Mirkovic J, Kissel E. Comparative evaluation of spoofing defenses. IEEE Trans. on Dependable and Secure Computing, 2011,8(2):218−232. [doi: 10.1109/TDSC.2009.44]

[64] Liu B, Bi J, Vasilakos A. Toward incentivizing anti-spoofing deployment. IEEE Trans. on Information Forensics and Security, 2014,9(3):436−450. [doi: 10.1109/TIFS.2013.2296437]

[65] Liu BY, Bi J. On the deployability evaluation model of Internet Inter domain source address validation. Chinese Journal of Computers, 2015,38(3):500−514 (in Chinese withEnglish abstract). [doi: 10.3724/SP.J.1016.2015.00500]

[66] Liu B, Bi J, Zhou Y. Source address validation in software defined networks. In: Proc. of the 2016 Conf. on ACM SIGCOMM 2016 Conf. ACM Press, 2016. 595−596. [doi: 10.1145/2934872.2960425]

[67] Yu M, Zhang Y, Mirkovic J. SENSS: Software defined security service. In: Open Network Summit (ONS). Santa Clara, 2014. https://www.usenix.org/system/files/conference/ons2014/ons2014-paper-yu.pdf

[68] Lepinski M, Kent S. An infrastructure to support secure internet routing. RFC 6480, 2012.

[69] Huston G, Loomans R, Michaelson G. A profile for resource certificate repository structure. RFC 6481, 2012.

[70] Lepinski M, Kent S, Kong D. A profile for route origin authorizations (ROAs). RFC 6482, 2012.

[71] Liu B, Bi J, Yang X. FaaS: Filtering ip spoofing traffic as a service. ACM SIGCOMM Computer Communication Review, 2012, 42(4):113−114. [doi: 10.1145/2377677.2377707]

[72] Gill P, Schapira M, Goldberg S. Let the market drive deployment: A strategy for transitioning to BGP security. ACM SIGCOMM Computer Communication Review, 2011,41(4):14−25. [doi: 10.1145/2043164.2018439]

附中文参考文献:

[4] 吴建平,林嵩,徐恪,刘莹,朱敏.可演进的新一代互联网体系结构研究进展.计算机学报,2012,35(6):1094−1108. [doi: 10.3724/SP.J.1016.2012.01094]

[5] 吴建平,吴茜,徐恪.下一代互联网体系结构基础研究及探索.计算机学报,2008,31(9):1536−1548. [doi: 10.3321/j.issn:0254-4164.2008.09.007]

[6] 徐恪,朱亮,朱敏.互联网地址安全体系与关键技术.软件学报,2014,25(1):78−97. http://www.jos.org.cn/1000-9825/4509.htm [doi: 10.13328/j.cnki.jos.004509]

[8] 黎松,诸葛建伟,李星.BGP 安全研究.软件学报,2013,24(1):121−138. http://www.jos.org.cn/1000-9825/4346.htm [doi: 10.3724/SP.J.1001.2013.04346]

[9] 王娜,杜学绘,王文娟,刘敖迪.BGP 安全研究综述.计算机学报,2016,39. http://www.cnki.net/kcms/detail/11.1826.TP.20160920.2102.004.html [doi: 10.11897/SP.J.1016.2017.01626]

[40] 刘冰洋.互联网域间源地址验证的可部署性评价模型与方法设计[博士学位论文].北京:清华大学,2014.

[46] 王立军,吴建平,徐恪.支持域间分布式分组过滤的 BGP 扩展.软件学报,2007,18(12):3048−3059. http://www.jos.org.cn/1000-9825/20071208.htm

[52] 吴建平,任罡,李星.IPv6 网络自治系统间源地址验证技术研究.中国科技论文在线,2007,2(10):715−719. [doi: 10.3969/j.issn.2095-2783.2007.10.003]

[53] 范琪琳,尹浩,林闯,董加卿,宋伟.互联网自治域商业关系推测算法.计算机学报,2014,37(4):950−962. [doi: 10.3724/SP.J.1016.2014.00950]

[57] 姚广.基于路径的互联网源地址验证研究[博士学位论文].北京:清华大学,2011.

[65] 刘冰洋,毕军.互联网域间源地址验证的可部署性评价模型.计算机学报,2015,38(3):500−514. [doi: 10.3724/SP.J.1016.2015.00500]

贾溢豪(1991－),男,四川成都人,博士生,主要研究领域为计算机网络,下一代互联网体系结构,域间源地址验证.

刘莹(1973－),女,博士,副研究员,博士生导师,CCF 高级会员,主要研究领域为计算机网络,下一代互联网体系结构.

任罡(1979－),男,博士,助理研究员,主要研究领域为计算机网络体系结构,下一代互联网,网络安全.