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.