完成.DDNS 的特点是继承了 DHash 的容错和负载均衡等特性.在负载均衡方面,使用一致性哈希来给每个阶段平均分配秘钥,在每个节点被检索的同时,缓存查询路径,这种查询方法的时间复杂度为 $O(\log N)$.在鲁棒性方面,随着服务器的加入和退出,分布式哈希表自动转移数据,所以这些数据总会存储在固定数量的服务器上.由于这些服务器以伪随机的方式进行选取,只有所有的服务器同时瘫痪后,数据才会发生丢失.P-DONAS 将每个域名供应商(ISP)的站点作为接入节点 AN(access node).这些 AN 负责与客户端交互,并且也负责存储资源记录.经常被用户访问的 AN 被称为触发节点(triggering node),当收到用户请求时,触发节点首先查找自己的缓存记录,如果没有找到就在 P2P 网络上进行查找,如果仍没有找到,P-DONAS 就会查询传统的 DNS 服务,如果查询到结果,则将结果返回给 AN,AN 将结果返回给客户端,并在缓冲区进行缓存.如果在传统 DNS 服务器上仍未找到结果,则返回记录不存在或超时结束查询.当 P-DONAS 系统内没有缓存记录时,就查找传统 DNS 服务器,因此,P-DONAS 与传统的 DNS 服务器也是兼容的.

为了提高基于分布式哈希表域名系统的检索效率,基于 Beehive[67]主动缓存机制可以实现平均查找时间复杂度为 $O(1)$,并支持快速更新.CoDoNS[68]系统采用这种设计思想,并可与传统的 DNS 系统兼容,实现平滑过渡.CoDoNS 由全球的分布式节点组成,这些节点自组织形成一个 P2P 网络,通过家点(home node)来缓存域名记录,如果家节点失效,则其相邻节点就会成为家节点.CoDoNS 采用与传统 DNS 一样的协议和传输形式,客户端解析器不需要修改.CoDoNS 将命名空间的管理从传统 DNS 中分离,域名拥有者只需从域名提供商那里购买名字证书,域名供应商就可以将他们加入到 CoDoNS,域名拥有者也不需要为域名提供专用的服务器.CoDoNS 的查询解析过程很简单,客户端向 CoDoNS 发送 DNS 查询请求,CoDoNS 在家节点获得记录或在中间节点获得缓存记录,向客户端发送应答信息.除此之外,家节点会与传统的 DNS 服务器进行交互,保持存储的记录是最新的,并更新缓存信息.

基于 P2P 的 DNS 系统易受网络环境影响,当网络波动时查询效率会降低.为了解决传统 DNS 的结构问题和基于 P2P 网络的效率问题,HDNS[69]将 P2P 与传统 DNS 系统结合,提出一种混合结构 DNS 系统的方案.该系统分为两个部分:共有区(public zone),节点用 P2P 网络组织;内部区(internal zone),节点用传统 DNS 的树形结构组织.所有的共有区中的节点被分配一个唯一标识符,内部区树形结构中的根节点也分配一个唯一标识符,并将根节点标识符与共有区的标识符进行映射.以这种方式,每个内部区和共有区进行关联.鉴于效率和安全性能,在公有区存储顶级域名和二级域名,其余部分存储在内部区.查询时首先在共有区查询顶级域名和二级域名的标识符,通过映射得到内部区的根节点的标识,然后在该根节点下查找其余部分的记录,最终将查询结果返回.HDNS 由于采用混合结构,安全性比传统 DNS 要高,且查询速率比完全基于 P2P 网络的域名系统要快.虽然基于 P2P 网络的域名系统具有鲁棒性和负载均衡等优点,但是基于 P2P 网络的域名系统同样存在如下的局限性.

- 最坏情况下的查询延迟则不能接受:P2P 网络由于底层实现的不同有不同的处理延迟,但是最坏情况下的查询延迟则不能接受,如一条查询请求可能会在多个高延迟的网络上进行多次传播才被处理,解析效率明显降低.
- 节点信息更新导致状态不一致:P2P 网络允许任何节点修改数据.当一个节点修改完数据没有进行广播时就断开连接,将导致网络节点状态不一致,有些节点存储的还是过期的域名信息.
- 数据伪造:P2P 网络没有数据写入速率限制和接入控制机制,攻击者可以向整个 P2P 网络泛洪大量的垃圾数据,也可以伪造一些虚假的域名信息传播到整个网络.

3.4.2 基于区块链的域名结构

区块链是分布式数据存储、点对点传输、共识机制、加密算法等技术的新型应用模式.利用区块链去中心化、不可篡改、可追溯、高可信和多方维护的特点[70],为设计去中心化 DNS 提供了新思路.

Namecoin[71]是基于 Bitcoin[72]开发的 DNS 系统,在 Bitcoin 系统的基础上,将区块链存储的交易信息替换为名称-数值映射数据.因此,Namecoin 和 Bitcoin 有大多数共有的功能和机制,但 Namecoin 是一个更加通用的名称——数值对解析系统,而不是当前 DNS 系的替代.Namecoin 通过使用不同的前缀来匹配其他类型的名称——数值对.如“d/”前缀被用在域名,“id/”前缀被用在注册身份.Namecoin 使用虚拟.bit 顶级域名,但是这个域名没有

被官方注册到当前的 DNS 系统中,Namecoin 和 DNS 系统是隔离的,如果不安装附加的解析软件,则 DNS 系统不能解析.bit 中的域名.

Namecoin 底层由 Bitcoin 系统实现,只是将存储信息由交易数据替换为名称-数值映射信息,在扩展上存在局限性.为了解决 Namecoin 的扩展性问题,Blockstack[73]提出了将域名数据和控制分层的方案,域名记录存储在外部数据库中,而底层控制由区块链实现.Blockstack 在区块链中仅仅保存少量的元数据(即数据哈希和状态转变),并使用外部存储来存储实际大块数据.控制平面定义了注册协议、可读名字信息、创建名字哈希绑定和秘钥绑定.数据平面负责数据的存储和可用性保证.Blockstack 由 4 层组成,控制平面中包含区块链层、虚拟链层,数据平面中包含路由层和数据存储层.第 1 层的区块链层,负责存储区块链操作序列,并提供操作写入顺序的共识.第 2 层是虚拟化层,定义了新的操作,但并不需要更改底层的区块链层,只有 Blockstack 节点知道这些操作,而底层的区块链节点并不知道.此外,Blockstack 操作的接受和拒绝规则也定义在虚拟化层.第 3 层是路由层,Blockstack 从实际的存储数据中分离出路由请求,这避免了系统从一开始就采用任何特定的存储服务,取而代之的是允许多个存储提供商共存,包括商业云存储和 P2P 系统.如传统 DNS 使用区域文件(zone file)一样,Blockstack 也使用区域文件来存储路由信息.第 4 层的存储层在最顶层,它存储名称-数值对的实际数据.所有的数据被各自所有者的秘钥签名.用户不需要信任存储层,因为它们可以验证控制平面中数据值的完整性.存储层有两种存储方式:可变存储和不可变存储,这两种方式的区别在于数据的完整性验证方面,Blockstack 支持这两种方式同时运行.此外,仍有多种基于区块链技术的比特币衍生系统,这些系统同样提供名字解析服务,如基于 ethereum 的 ens[74]、peername[75]、Emercoin 的 EMCDNS[76].基于区块链的域名系统也存在如下局限性.

- 与传统的 DNS 系统不兼容,客户端浏览器必须安装插件才能访问域名系统,因此基于区块链的域名系统很难大范围部署.
- Namecoin 和 Blockstack 的底层实现都是 Bitcoin.由于 Bitcoin 采用“one-CPU-one-vote”机制.如果某组织控制了整个系统 51%的算力,即 51%攻击,将会对系统造成严重的安全隐患.虽然 51%攻击是理论上的存在,但是如果拥有 25%的算力就可以威胁系统安全[77].
- 由于区块链存储所有历史信息,整个系统会变得越来越庞大,移动设备或个人电脑很难有足够的硬盘空间存下所有的记录信息.虽然有学者提出 SNV(simple name verification)协议[78],但是需要设置提供全部记录的服务器,服务器与客户端之间的通信安全又是一个需要解决的问题.

3.4.3 基于根服务器联盟的系统结构

DNS 系统的中心化解析蕴含着权利滥用的风险,即一个顶级域可能被删除,导致整个顶级域名下的子域名无法解析.为了解决 DNS 根服务器中心化问题,应从结构和解析机制两方面进行改进.

在根服务器结构方面,主要采用以下技术将根服务器去中心化[79]:(1) 递归根:在递归服务器上直接进行根区解析;(2) 伪装根:将到根区查询引导到镜像根服务解析;(3) 开放根:建立一组独立运作的根服务器,使用 IANA 的根区数据作为解析数据源;(4) 全球根:通过增加根服务器数量,采用任播技术,将 13 个根服务器扩展到更大规模.这 4 种方案中根区数据依然来自 IANA,权利滥用分析仍然存在.

在解析机制方面,采用域名对等扩散[80]的方式,即让各个顶级域名所有者向其他国家顶级域名掌握者报告顶级服务器的地址.域名对等扩散体系下的自主根和国际根服务器处于混合工作的状态,自主根将目前根服务器的中心化问题转移到了顶级域名服务器,但是,如果.com 一类的顶级域名服务器拒绝将权威信息转交给自主根,那么自主根将会受到很大限制.

将根服务器权利弱化为多个子节点,DDNS 系统[81]采用这种方式限制根服务器权利.DDNS 基于 Paxos[82]分布式一致性算法,分级分区域管理域名.根区的事务请求要得到过半根节点的投票才能通过,从而不依赖主根服务器.这种方案的本质是将根服务器的权限下放为各个子根,通过投票机制决定事务请求,但是这种设计的局限性是子根服务器会相互结盟,投票选举的结果受结盟的控制,从而影响正常的事务请求.

3.5 小 结

DNS 的安全形势严峻,为了应对各种 DNS 安全威胁,本节从协议增强、系统增强、检测监控、去中心化的

域名系统 4 个方面对当前 DNS 安全方案进行了总结.为了更加直观地分析并对比各种增强方案的优点和局限性,进行了比较分析.表 4 围绕客户端兼容性、协议向后兼容性、隐私性、抗 DoS 攻击、抵御缓存投毒攻击、延迟方面进行了归纳总结.

Table 4 Comparison of various DNS enhancement schemes

表 4 DNS 安全增强方案分析和比较

增强方案	内容	对比					
		协议兼容	与传统 DNS 兼容	隐私性	抗 DoS 攻击	抗缓存投毒	延迟低
协议增强	DNSSEC	√	√	×	×	√	×
	DNSCurve	√	√	√	Part	√	×
系统增强	T-DNS	×	×	√	×	√	×
	EncDNS	×	√	√	×	√	×
	CoDNS	√	√	×	√	Part	√
	CofiDNS	√	√	×	×	Part	√
	DR-DNS	√	√	×	×	×	×
P2P 结构	DDNS	×	×	×	√	√	×
	CoDoDNS	√	√	×	√	√	√
	P-DONAS	√	√	×	√	√	×
区块链结构	Namecoin	√	×	√	√	√	×
	Blockstack	√	×	√	√	√	×
	ENS	√	×	√	√	√	×
	peername	√	×	√	√	√	×
	EMCDNS	√	×	√	√	√	×

4 未来研究方向

针对 DNS 的各种安全问题,虽然涌现了大量的解决办法,但是近年来的各种攻击事件表明,DNS 安全问题仍然十分严峻.通过分析发现,现有的研究成果仍存在不足,未来的研究工作可以更多地关注以下几个方面.

4.1 去中心化DNS系统的研究

DNS 系统之所以受到各种攻击,与 DNS 树形结构、根服务器管理整个系统有重要关系.这种体系架构存在单点失效问题,而历史上有多次攻击根服务器的案例,致使整个 DNS 服务瘫痪.因此,设计一种去中心化的 DNS 系统是一项具有重要意义的研究课题[74−79,82,83].目前,针对去中心化 DNS 设计主要包含以下两个方向.

(1) 基于区块链技术.区块链技术的出现为去中心化设计提供技术和框架,利用区块链技术设计去中心化 DNS 系统也是一个新的研究思路.目前,该方式面临的主要挑战包括:

- 高效的 P2P 网络设计,P2P 网络面临的问题包括容易受到网络波动的影响,在网络波动剧烈的环境下,查询效率将会大大降低;数据伪造和缺乏接入控制使一些虚假信息传播到 P2P 网络[84].设计一种高效、安全的 P2P 网络是一个基于区块链去中心化 DNS 设计的重要课题.
- 高效的共识算法设计.目前主要的共识算法包括基于工作量证明、权益证明的方式,但是这些共识算法共识效率低,共识过程中会出现分叉,并不适合 DNS 数据的实时更新和维护,共识算法的设计需要结合 DNS 的应用场景设计,共识效率高、共识过程保证中保证强一致性,保证每个节点存储数据一致.

(2) 基于根服务器联盟的方式.这种方案的主要研究思路是不同国家或不同的顶级服务器通过联盟的方式,降低根服务器中心化控制.这种方式面临的挑战包括国家根联盟体系结构设计、根联盟系统的控制、根联盟与主根服务器的同步问题.

4.2 开放式DNS服务器安全检测

虽然开放式服务器提供了各种便利,如可以应答外部资源的 DNS 请求,但是这些开放系统给网络的安全性和稳定性带来了极大的隐患.一些开放的服务器容易被攻击者控制,实施放大攻击、投毒攻击等恶意行为.据调查发现,在 3 200 万个开放式解析器中有 2 800 万存在严重的安全隐患.开放式会给攻击者进行 DoS/DDoS、缓冲投毒、DNS ID 劫持等攻击带来便利.现有的研究中很少有对这些开放式系统进行规范和研究,如何识别和监控这些恶意的开放式服务器,也是一个重要的研究课题.目前面临的主要挑战包括:

(1) 现有的大多数检测系统检测对象单一,在实际应用中不能为检测某种恶意行为就配置一种检测系统,因此有必要构建一种综合的检测系统,能够有效地监测各种安全威胁.

(2) 当前无论是基于机器学习、信息熵,还是统计分析等理论方法,都难以抵御特殊类型的攻击,如利用软件的零日漏洞发起的攻击.现有的检测系统检测效率还有待提高,对于像 DNS 隧道、隐私泄露等检测并不能在信息泄露时得到及时发现,因此新的检测系统也要满足及时性要求.

4.3 防护方案增量部署

由于 DNS 系统的广泛应用,有学者虽然提出了改进方案,但与现有的 DNS 系统仍不够兼容,也很难被大范围部署.DNSSEC 虽然在 1997 年就已被提出,但是目前仍未广泛部署,截至 2016 年 12 月,虽然 DNSSEC 在顶级域的部署率达到了 89%,但在二级域的部署率仅为 3%[85].有很多新型的名字服务系统和架构均已提出,但与当前 DNS 系统仍不够兼容,因此,这些研究成果很难被网络运营商和大型公司所采用.因此在设计防护方案的部署方式时,应考虑防护方案要避免修改现有 DNS 协议.

4.4 云环境下的DNS安全检测与隐私保护

互联网基础设施正迅速向私有/公共云混合模型转变.云服务正被广泛使用,有 93%的组织使用软件、基础设施或平台作为服务对象.虽然云服务带来了很大的便利,但是仍有 42%的组织受到了直接来自 DNS 的云应用宕机攻击,这种攻击对象包括共有云和私有云.在云环境下,DNS 安全面临以下问题.

(1) 云环境下的 DNS 安全检测.目前 DNS 检测主要针对 ISP 下 DNS 服务器之间的流量,对于云环境中的 DNS 服务器的检测研究成果较少,但是近年来,云环境下的 DNS 安全十分严峻,因此,如何设计和检测云服务下 DNS 安全问题是一个可探索的方向.

(2) 云环境下基于 DNS 的隐私泄露检测.云环境用户隐私数据泄露十分严重[86],如利用 DNS 隧道的方式进行隐私数据的传输和窃取.如何检测云环境下 DNS 数据隐私泄露问题也非常值得关注.

5 总 结

DNS 作为互联网重要的基础设施,从早期的 DNS 协议安全增强,到现在的体系结构改进,其安全防护问题一直是学术界和工业界所关心的问题.本文对 DNS 安全防护技术进行了全面的分析和总结,同时对未来可能的研究热点进行了介绍,为进一步研究提供参考.

致谢 感谢本文的匿名评阅专家对文章内容、分类方法的完善提出的许多建设性意见和建议,同时对《软件学报》编辑老师的工作一并表示感谢

References:

[1] Hansen T, Hallambaker P. DomainKeys identified mail (DKIM) service overview. Baker, 2009.
[2] Tom L. Improving performance on the Internet. Communications of the ACM, 2009,52(2):44–51.
[3] Levine J. DNS blacklists and whitelists. IETF RFC 5782, 2010.
[4] Almeida VAF, Doneda D, Abreu JDS. Cyberwarfare and digital governance. IEEE Internet Computing, 2017,21(2):68–71.
[5] Chinese CN. https://www.computerworld.com/article/2484097/internet/major-ddos-attacks--cn-domain
[6] Turkey DNS. https://blog.radware.com/security/2015/12/turkey-dns-servers-under-attack/
[7] Bortzmeyer S. DNS privacy considerations. RFC 7626, 2015.
[8] Framework POS. https://www.anomali.com/blog/three-month-frameworkpos-malware-campaign-nabs-43000-credits-cards-from-poi
[9] Research RFC. https://www.rfc-editor.org/search/rfc_search_detail.php?title=DNS&pubstatus%5B%5D=Any&pub_date_type=any
[10] UDNS threat survey 2017. 2017. http://www.efficientip.com/resources/white-paper-dns-security-survey-2017/
[11] Anstee D, Bowen P, Chui CF, Sockrider G. In: Proc. of the 12th Worldwide Infrastructure Security Report. Arbor Network, 2017.

[12] Marc K, Hupperich T, Rossow C, *et al*. Exit from Hell? Reducing the impact of amplification DDoS attacks. In: Proc. of the USENIX. USENIX Association, 2014. 111–125.

[13] Cisco 2017 Midyear Cybersecurity Report. https://www.cisco.com/c/m/en_au/products/security/offers/cybersecurity-reports.html

[14] Wang Y, Hu M, Li B, *et al*. Survey on domain name system security. Journal on Communications, 2007,28(9):91–103 (in Chinese with English abstract).

[15] Hu N, Deng P, Yao S, *et al*. Issues and challenges of Internet DNS security. Chinese Journal of Network and Information Security, 2017,3(3):13–21 (in Chinese with English abstract).

[16] Jiang J. Research on inconsistent and multiple dependence in the authorization mechanism of Internet domain name system [Ph.D. Thesis]. Tsinghua University, 2013 (in Chinese with English abstract).

[17] Liu Q. The security of Internet domain name system in China. Modern Telecommunications Technology, 2010,2010(4):9–11 (in Chinese with English abstract).

[18] Li J. Detection of DNS spoofing and cache poisoning attacks [MS. Thesis]. Chengdu: University of Electronic Science and Technology of China, 2015 (in Chinese with English abstract).

[19] Schomp K, Callahan T, Rabinovich M, *et al*. Assessing DNS vulnerability to record injection. In: Proc. of the Int'l Conf. on Passive and Active Measurement. 2014. 214–223.

[20] Mohaisen A. Evaluation of privacy for DNS private exchange. IETF Internet Draft, 2015-05.

[21] Bortzmeyer S. DNS privacy considerations. IETF RFC 7626, 2015.

[22] Rossebo J, Cadzow S, Sijben P, *et al*. A threat, vulnerability and risk assessment method and tool for Europe. In: Proc. of the Int'l Conf. on Availability, Reliability and Security. 2007. 925–933.

[23] Banse C, Herrmann D, Federrath H. Tracking users on the Internet with behavioral patterns: Evaluation of its practical feasibility. In: Information Security and Privacy Research. Berlin, Heidelberg: Springer-Verlag, 2012. 235–248.

[24] Ariyapperuma S, Mitchell CJ. Security vulnerabilities in DNS and DNSSEC. In: Proc. of the 2nd Int'l Conf. on Availability, Reliability and Security. 2007. 335–342.

[25] Schomp K, Callahan T, Rabinovich M, *et al*. On measuring the client-side DNS infrastructure. In: Proc. of the Conf. on Internet Measurement. 2013. 77–90.

[26] Callahan T, Allman M, Rabinovich M. On modern DNS behavior and properties. ACM SIGCOMM Computer Communication Review, 2013,43(3):7–15.

[27] Shulman H, Waidner M. Towards security of Internet naming infrastructure. In: Proc. of the Computer Security-ESORICS. 2015.

[28] DNS Server Software Distribution. https://ftp.isc.org/www/survey/reports/2017/07/fpdns.txt

[29] Bind security vulnerabilities. CVE-2019-6465, 2019.

[30] Microsoft DNS server vulnerability. https://support.microsoft.com/en-us/help/2678371/microsoft-dns-server-vulnerability-to-dns-server-cache-snooping-attack

[31] Learn more at National vulnerability database (NVD). CVE-2017-11779, 2017.

[32] Microsoft Windows DNS server denial of service vulnerability. https://tools.cisco.com/security/center/viewAlert.x?alertId=53604

[33] Microsoft Windows DNS server cache poisoning vulnerability. https://www.securityfocus.com/bid/30132/

[34] Yeti DNS project. https://yeti-dns.org/

[35] Ateniese G, Mangard S. A new approach to DNS security (DNSSEC). In: Proc. of the 8th ACM Conf. on Computer and Communications Security. 2001. 86–95.

[36] Yang H, Osterweil E, Massey D, Lu SW, Zhang LX. Deploying cryptography in Internet-scale systems: A case study on DNSSEC. IEEE Trans. on Dependable and Secure Computing, 2011,8:656–669.

[37] Herzberg A, Shulman H. DNSSEC: Interoperability challenges and transition mechanisms. In: Proc. of the 7th Int'l Conf. on Availability, Reliability and Security. 2013. 398–405.

[38] Herzberg A, Shulman H. DNSSEC: Security and availability challenges. In: Proc. of the Communications and Network Security. 2013. 365–366.

[39] Lian W, Rescorla E, Shacham H, *et al*. Measuring the practical impact of DNSSEC deployment. In: Proc. of the USENIX Security. 2013. 573–588.

[40] Dempsky M. DNSCurve: Link-level security for the domain name system. Internet Draft draft-dempsky-dnscurve-01, RFC, 2010.

[41] Anagnostopoulos M, Kambourakis G, Konstantinou E, Gritzalis S. DNSSEC vs. DNSCurve: A side-by-side comparison. In: Proc. of the IGI Global. 2012. 201–220.

[42] Zhu L, Hu Z, Heidemann J, *et al*. Connection-oriented DNS to improve privacy and security. In: Proc. of the ACM Conf. on SIGCOMM. 2015. 379–380.

[43] Shulman H. Pretty bad privacy: Pitfalls of DNS encryption. In: Proc. of the Workshop on Privacy in the Electronic Society. 2014. 191–200.

[44] Park K, Pai VS, Peterson L, *et al*. CoDNS: Improving DNS performance and reliability via cooperative lookups. In: Proc. of the 6th Symp. on Operating Systems Design and Implementation. San Francisco, 2004. 14.

[45] Poole L, Pai VS. ConfiDNS: Leveraging scale and history to improve DNS security. In: Proc. of the 3rd Workshop on Real, Large Distributed Systems (WORLDS). 2006.

[46] Khurshid A, Kiyak F, Caesar M. Improving robustness of DNS to software vulnerabilities. In: Proc. of the 27th Annual Computer Security Applications Conf. Orlando, 2011. 177–186.

[47] Huang K, Kong N. Research on status of DNS privacy. Computer Engineering and Applications, 2018,54(9):28–36 (in Chinese with English abstract).

[48] Scaife N, Carter H, Traynor P. OnionDNS: A seizure-resistant top-level domain. In: Proc. of the Communications and Network Security. 2015. 379–387.

[49] Herrmann D, Fuchs K, Lindemann J, *et al*. EncDNS: Alightweight privacy-preserving name resolution service. In: Proc. of the Computer Security-ESORICS 2014. 2014. 37–55.

[50] Choi H, Lee H, Kim H. BotGAD: Detecting botnets by capturing group activities in network traffic. In: Proc. of the 4th Int'l ICST Conf. on Communication System Software and Middleware. ACM, 2009. 2.

[51] Choi H, Lee H. Identifying botnets by capturing group activities in DNS traffic. Computer Networks, 2012,56(1):20–33.

[52] Babak R, Perdisci R, Antonakakis M. Segugio: Efficient behavior-based tracking of malware-control domains in large ISP networks. In: Proc. of the Int'l Conf. on Dependable Systems and Networks. IEEE, 2015. 403–414.

[53] Perdisci R, Corona I, Dagon D, Lee W. Detecting malicious flux service networks through passive analysis of recursive DNS traces. In: Proc. of the Annual Computer Security Applications Conf. (ACSAC 2009). IEEE, 2009. 311–320.

[54] Huang SY, Mao CH, Lee H M. Fast-flux service network detection based on spatial snapshot mechanism for delay-free detection. In: Proc. of the 5th ACM Symp. on Information, Computer and Communications Security. 2010. 101–111.

[55] Yadav S, Reddy AN. Winning with DNS failures: Strategies for faster botnet detection. In: Rajarajan M, Piper F, Wang H, Kesidis G, eds. Security and Privacy in Communication Networks. Berlin, Heidelberg: Springer-Verlag, 2012. 446–459.

[56] Dong LP, Chen XY, Yang YJ, *et al*. Implementation and detection of network covert channel. Computer Science, 2015,42(7): 216–244 (in Chinese with English abstract).

[57] Antonakakis M, Perdisci R, Dagon D, *et al*. Building a dynamic reputation system for DNS. In: Proc. of the USENIX Security. 2010. 18–36.

[58] Bilge L, Kirda E, Kruegel C, *et al*. EXPOSURE: Finding malicious domains using passive DNS analysis. In: Proc. of the Network and Distributed System Security Symp. (NDSS 2011). 2011.

[59] Antonakakis M, Perdisci R, Lee W, *et al*. Detecting malware domains at the upper DNS hierarchy. In: Proc. of the 20th USENIX Conf. on Security. 2011. 21–27.

[60] Bishop CM. Pattern Recognition and Machine Learning (Information Science and Statistics). New York: Springer-Verlag, 2006.

[61] Zhang WW, Gong J, Liu SD, Hu XY. DNS surveillance on backbone. Ruan Jian Xue Bao/Journal of Software,2017,28(9): 2370−2387 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5186.htm [doi: 10.13328/j.cnki.jos.005186]

[62] Dabek F, Kaashoek MF, Karger D, Morris R, Stoica I. Wide-area cooperative storage with CFS. In: Proc. of the ACM Symp. on Operating Systems Principles (SOSP 2001). Chateau Lake Louise, 2001.

[63] Stoica I, Morris R, Karger D, *et al*. Chord: A scalable peer-to-peer lookup service for Internet applications. IEEE/ACM Trans. on Networking, 2003,11(1):17–32.

[64] Cox R, Muthitacharoen A, Morris R. Serving DNS using a peer-to-peer lookup service. In: Proc. of the 1st Int'l Workshop on Peer-to-Peer Systems. Cambridge, 2002. 155–165.

[65] Maymounkov P, Mazières D. Kademlia: A peer-to-peer information system based on the XOR metric. In: Proc. of the 1st Int'l Workshop on Peer-to-Peer Systems (IPTPS 2001). London: Springer-Verlag, 2002. 53–65.

[66] Danielis P, Altmann V, Skodzik J, Wegner T, Koerner A, Timmermann D. P-DONAS: A P2P-based domain name system in access networks. ACM Trans. on Internet Technology, 2015,15(3):11.

[67] Ramasubramanian V, Sirer EGU. Beehive: $O(1)$ lookup performance for power-law query distributions in peer-to-peer overlays. In: Proc. of the 1st Conf. on Networked Systems Design and Implementation. San Francisco, 2004.

[68] Ramasubramanian V, Sirer EGU. The design and implementation of a next generation name service for the Internet. In: Proc. of the 2004 Conf. on Applications, Technologies, Architectures, and Protocols for Computer Communications. 2004. 331–342.

[69] Song Y, Koyanagi K. Study on a hybrid P2P based DNS. In: Proc. of the IEEE Int'l Conf. on Computer Science and Automation Engineering. Shanghai, 2011. 152–155.

[70] Tsai WT, Yu L, Wang R, Liu N, Deng EY. Blockchain application development techniques. Ruan Jian Xue Bao/Journal of Software, 2017,28(6):1474−1487 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5232.htm [doi: 10.13328/j.cnki.jos.005232]

[71] Namecoin. https://Namecoin.info

[72] Satoshi N. Bitcoin: A peer-to-peer electronic cash system. 2009.

[73] Ali M, Nelson J, Shea R, *et al*. Blockstack: A global naming and storage system secured by block chains. In: Proc. of the 2016 USENIX Annual Technical Conf. (USENIX ATC 16). 2016. 181–194.

[74] ENS. https://ens.domains/

[75] PeerName. https://peername.com/

[76] EMCDNS. https://emercoin.com/

[77] Eyal I, Sirer EG. Majority is not enough: Bitcoin mining is vulnerable. In: Proc. of the Financial Cryptography. 2014.

[78] Simplified name verification protocol. https://blockstack.org/

[79] Zhang Y, Xia CD, Fang BX, *et al*. An autonomous open root resolution architecture for domain name system in the Internet. Journal of Cyber Security, 2017,2(4) (in Chinese with English abstract).

[80] Fang BX. Discussion on autonomous root domain name system based on national union from "Network Sovereignty". Information Security and Communications Privacy, 2014(12):35–38 (in Chinese with English abstract).

[81] Zhu GK, Jiang WB. A decentralized domain name system for the network. Cyberspace Security, 2017,8(1):14–18 (in Chinese with English abstract).

[82] Lamport L. The part-time parliament. ACM Trans. on Computer Systems, 1998,16(2):133–169.

[83] Open resolver project. 2016. http://openresolverproject.org/

[84] Lu ZH, Gao XH, Huang SJ, *et al*. Scalable and reliable live streaming service through coordinating CDN and P2P. In: Proc. of the Int'l Conf. on Parallel and Distributed Systems. IEEE, 2012. 581–588.

[85] DNSSEC deployment report. http://rick.eng.br/dnssecstat/

[86] Bhadauria R, Sanyal S. Survey on security issues in cloud computing and associated mitigation techniques. arXiv Preprint arXiv:1204.0764, 2012.

附中文参考文献:

[14] 王垚,胡铭曾,李斌,等.域名系统安全研究综述.通信学报,2007,28(9):91–103.

[15] 胡宁,邓文平,姚苏.互联网 DNS 安全研究现状与挑战.网络与信息安全学报,2017,3(3):13–21.

[16] 江健.互联网域名系统授权机制中不一致和多重依赖问题研究[博士学位论文].北京:清华大学,2013.

[17] 柳青.我国互联网域名系统的安全问题.现代电信科技,2010,2010(4):9–11.

[18] 李杰.DNS 欺骗和缓存中毒攻击的检测[硕士学位论文].成都:电子科技大学,2015.

[47] 黄锴,孔宁.DNS 隐私问题现状的研究.计算机工程与应用,2018,54(9):28–36.

[56] 董丽鹏,陈性元,杨英杰,等.网络隐蔽信道实现机制及检测技术研究.计算机科学,2015,42(7):216–244.

[61] 张维维,龚俭,刘尚东,胡晓艳.面向主干网的 DNS 流量监测.软件学报,2017,28(9):2370−238. http://www.jos.org.cn/1000-9825/5186.htm [doi: 10.13328/j.cnki.jos.005186]

[70] 蔡维德,郁莲,王荣,刘娜,邓恩艳.基于区块链的应用系统开发方法研究.软件学报,2017,28(6):1474–1487. http://www.jos.org.cn/1000-9825/5232.htm [doi: 10.13328/j.cnki.jos.005232]

[79] 张宇,夏重达,方滨兴,张宏莉.一个自主开放的互联网根域名解析体系.信息安全学报,2017,2(4):57–69.

[80] 方滨兴.从“国家网络主权”谈基于国家联盟的自治根域名解析体系.信息安全与通信保密,2014,(12):35–38.

[81] 朱国库,蒋文保.一种去中心化的网络域名服务系统模型.网络空间安全,2017,8(1):14–18.

王文通(1994－),男,硕士,主要研究领域为网络安全,网络通信,数据中心网络.

胡宁(1972－),男,博士,博士生导师,CCF 专业会员,主要研究领域为网络安全,软件定义网络,机器学习.

刘波(1973－),男,博士,博士生导师,CCF 专业会员,主要研究领域为网络空间安全,大数据分析.

刘欣(1978－),男,博士,CCF 专业会员,主要研究领域为计算机网络,软件工程.

李树栋(1979－),男,博士,CCF 专业会员,主要研究领域为网络空间安全.