软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software, [doi: 10.13328/j.cnki.jos.006046]

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

DNS 安全防护技术研究综述*

王文通[1,2], 胡 宁[1], 刘 波[2], 刘 欣[3], 李树栋[1]

[1](广州大学 网络空间先进技术研究院,广东 广州 510006)

[2](国防科技大学 计算机科学与技术学院,湖南 长沙 410073)

[3](长沙学院, 计算机工程与应用数学学院,湖南 长沙 410022)

通讯作者: 胡宁, E-mail: huning@gzhu.edu.cn;刘欣, E-mail: xin.liu@ccsu.edu.cn;

摘 要: DNS 为互联网应用提供名字解析服务,是互联网的重要基础服务设施. 近年发生的互联网安全事件表明 DNS 正面临严峻的安全威胁.DNS 的安全脆弱性主要包括:协议设计脆弱性、技术实现脆弱性和体系结构脆弱性. 针对上述脆弱性,对 DNS 协议设计、系统实现、检测监控和去中心化等方面的最新研究成果进行了归纳和总结, 并且对未来可能的热点研究方向进行了展望.

关键词: DNS 安全; DNS 脆弱性; DNS 安全增强; DNS 去中心化;

中图法分类号: TP311

中文引用格式: 王文通, 胡宁, 刘欣, 李树栋, 刘波. DNS 安全防护技术研究综述. 软件学报,2020. http://www.jos.org.cn/1000-9825/6046.htm

英文引用格式: Wang WT, Hu N, Liu X, Li SD, Liu B. A Survey on Technology of Security Enhancement for DNS. Ruan Jian Xue Bao/Journal of Software, (in Chinese). http://www.jos.org.cn/1000-9825/6046.htm

A Survey on Technology of Security Enhancement for DNS

WANG Wen-Tong[1,2], HU Ning[1], LIU Xin[2], LI Shu-Dong[2], LIU Bo[2]

[1](Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China)

[2](School of Computer Science and Technology, National University of Defense of Technology, Changsha 410073, China)

[3](School of Computer Engineering and Applied Mathematics, Changsha University, Changsha 410022, China)

Abstract: As a vital infrastructure of the Internet, DNS provides name resolution services for Internet applications. Major Internet incidents in recent years indicate that DNS is facing serious security threats. The vulnerability of DNS can be divided into three categories: protocol design vulnerability, technology implementation vulnerability, and architecture vulnerability. In view of the above vulnerabilities, the latest research achievements on DNS security enhancement are summarized which include protocol design, system implementation, DNS monitoring and DNS decentralization. Some possible future research hotspots and challenges are also discussed.

Key words: DNS security; DNS vulnerability; DNS Security Enhancement; DNS decentralization

域名系统(DNS, Domain Name System)作为互联网的重要基础设施,其主要功能是提供域名解析服务.随着互联网的发展,DNS 也被赋予了其他的应用功能,如 DKMI 标准[1] (Domain Keys Identified Mail, DKIM)、负载均衡[2] 、域名封锁[3] 等方面.互联网的大多数应用都需要依赖 DNS 才能正常工作,一旦 DNS 系统受到攻击, 整个互联网将会受到严重影响.

* 基金项目:国家自然科学基金(61976064,61672020,61572513), 国防科技创新特区项目(18-H863-01-ZT-005-027-02),装备预研重点实验室基金项目(61421030203).

Foundation item: National Natural Science Foundation of China (61976064, 61672020, 61572513), National Defense Science and technology innovation special zone project(18-H863-01-ZT-005-027-02), Equipment Pre-Research Key Laboratory Fund Project (61421030203).

收稿时间: 2018-06-12; 修改时间: 2018-10-15, 2020-01-07; 采用时间: 2020-03-28; jos 在线出版时间: 2020-04-21

目前实际使用的 DNS 协议主要遵循 RFC1034 和 RFC1035 规范,为了弥补 DNS 协议缺乏信息校验的不足,RFC4034 引入了基于 PKI 技术的 DNSSEC 增强方案.然而,DNS 系统的安全威胁并未因此减弱.近年来的各种 DNS 安全事件[4-6],不仅对被攻击的组织和公司造成严重的经济损失,也给整个互联网的稳定性带来严重的影响.随着一些新型攻击方法的出现,DNS 的安全环境变得更加严峻,例如:利用物联网设备对 DNS 系统发起 DDoS (distributed denial-of-attack)攻击[5] 、利用 DNS 报文分析用户的隐私信息[7] 、利用 DNS 建立隧道攻击[8] .

针对 DNS 的各种安全威胁,截止至 2017 年 12 月份,有关 DNS 的 RFC 文档多达 256 篇[9] .国内外学者针对 DNS 安全问题提出了许多新颖的思路.本文针对近 10 年来 DNS 安全威胁与防护相关研究工作进行了分析和综述,总结了 DNS 威胁的种类和原因,并侧重介绍 DNS 在协议、系统实现、诊断监测、隐私保护、体系结构方面的安全增强方法和研究进展,并结合区块链技术的不易篡改、多方维护、可溯源等特点,列举利用区块链技术设计去中心的域名系统的相关研究,并希望为未来的研究工作提供帮助和参考.

本文第 1 节介绍了 DNS 的安全现状.第 2 节对 DNS 的威胁进行分类,总结归纳 DNS 系统脆弱性的根本原因.第 3 节针对 DNS 系统脆弱性,列举各种安全增强方案,并进行比较分析.第 4 节对 DNS 安全研究工作提出热点和展望.最后作简要总结.

1 DNS 安全现状

随着网络技术的不断发展,攻击 DNS 的技术也变得更加丰富,手段更加复杂.美国 Coleman Parkes 公司调查了来自北美、亚太、欧洲共 1000 个组织的 DNS 系统安全状况发现[10] ,在 2017 年有 76%的组织受到了 DNS 攻击,在这些攻击中,恶意软件攻击占 35%、DDoS 攻击占 32%、缓存投毒占 23%、DNS 隧道占 22%、零日漏洞攻击占 19%.超过 90%的恶意软件使用 DNS 协议与恶意软件的命令和控制(command and control, C&C)中心保持联系,以此获取攻击命令、下载软件更新、获取隐私信息. DDoS 攻击也变得越来越复杂,攻击者使用广泛的技术手段,从基本的方法(如:放大/转发、泛洪),到涉及僵尸网络、连锁反应等高度复杂的攻击,这些攻击可能来内部或外部 DNS 服务器.根据 Arbor Network 发布的调查报告[11] 显示,有 84%的反射和放大攻击采用 DNS 协议,是所有调查协议中占比最高的.此外,报告中还显示 DNS 的服务器是 DDoS 攻击的首要目标,有 78%的 DDoS 攻击对 DNS 的应用层服务进行攻击.

攻击 DNS 有利可图,商业利益驱动促使攻击行为加剧.有攻击者通过攻击 DNS 服务器,造成企业服务中断,损坏企业信誉,造成用户流失.如 2016 年 10 月在 Dyn 域名服务供应商受到大规模 DDoS 攻击之后,Dyn 公司失去了 8%的域名客户.DNS 攻击还会造成关键数据泄露和经济损失.根据 EfficientIP 的调查报告,在调查的 1000 个公司和组织中,有三分之一的公司因 DNS 攻击数据被盗,这些数据中 16%是用户敏感信息,15%是知识产权信息.此外,DNS 攻击每年会给受害公司造成 200 万美元的经济损失.

DNS 攻击技术越来越丰富,但是与之应对的检测技术则比较匮乏.据 Cisco 的研究报告[13] 显示,攻击者通过恶意软件,在 24 小时内可以控制超过 10 万台物联网设备,通过这些物联网设备可以发动大规模的 DDoS 攻击.因为这些恶意软件被存储在受害设备的内存中,设备关机后就自动清除,很难收集恶意程序的样本,服务器软件的零日漏洞存在使检测检测难度增大,有 83%的公司没有及时安装安全补丁,导致攻击效果进一步加剧.

2 安全威胁分析

2.1 DNS层级关系及漏洞分析

DNS 主要由 3 部分组成,分别是:1)域名空间(domain name space)和资源记录(resource record),包括树形结构的命名空间和与名称相关联的数据;2)名字服务器(name server),包含域树结构信息和设置信息的服务器程序;3)解析器(resolver),响应请求并从名称服务器获取查询结果. DNS 通常提供两种域名解析方式，分别是：递归式查询和迭代式查询。在通常情况下，应用系统主机向本地域名服务器请求域名解析时，采用递归查询。在递归查询模式下，本地域名服务器直接向应用系统主机返回域名解析结果。当地域名服务器需要向根域名

服务器请求域名解析服务时，采用迭代查询。在迭代查询模式下，本地域名服务器需要与多台域名服务器交互，直至返回域名解析结果。DNS 的基本结构和工作原理如图 1 所示。

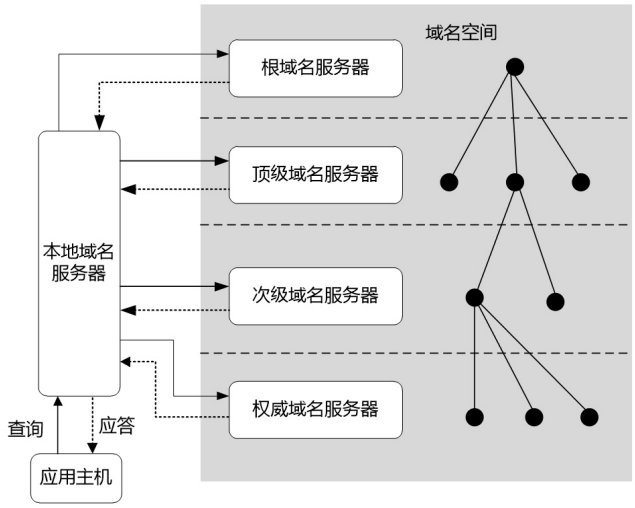

Fig.1 DNS architecture

图 1 DNS 体系结构

为了分析 DNS 不同服务器层级和协议的安全问题,本文对 CVE 漏洞信息库 623 条 DNS 相关漏洞进行对比分类，针不同类型的 DNS 系统漏洞对攻击目标及攻击后果进行总结归纳,统计结果如表 1 所示。

Table 1 Statistics of DNS vulnerabilities in CVE

表 1 CVE 中 DNS 漏洞统计

DNS 系统漏洞	攻击目标	攻击后果
资源消耗	DNS 服务器	拒绝服务
伪造 DNS 服务器流量	解析器	拒绝服务,信息泄露
报文处理能力缺失	服务器,解析器	拒绝服务
DNS 流量放大攻击	解析器	拒绝服务
DNSSEC 秘钥生成协议漏洞	DNS 协议	获得特权
异常报文导致缓冲区溢出	解析器,协议	获得特权
DNS 记录恶意更新	名称服务器	获得特权
绕过访问控制路径	服务器,解析器	获得特权
系统配置错误	服务器,解析器	拒绝服务,信息泄露
缓存投毒	服务器,协议	劫持,获得特权

2.2 DNS脆弱性分类

基于 DNS 漏洞和相关文献资料[15-18],本文将 DNS 的脆弱性概括为协议脆弱性、系统实现脆弱性、体系结构脆弱性.

2.2.1 协议脆弱性

DNS 协议在设计之初没有充分考虑网络安全问题,采用 UDP 协议传输信息,在消息传输的过程中,数据未经过加密处理,资源记录也不进行签名等防伪造保护.因此 DNS 协议很容易遭受缓存投毒、数据窃听、数据篡改等恶意攻击[14] .

对 DNS 记录缓冲区投毒是非常普遍的攻击方式[19] .互联网中存在大量的开放式解析器,为攻击者提供了更多的攻击目标,有实验表明有 7%~9%的解析器容易受到注入攻击.

DNS 协议还存在隐私泄露问题[20] [21] .由于 DNS 查询时包含许多敏感信息,在域名解析的过程中,可能会泄露用户身份和设备类型等个人隐私信息.有许多公司利用这一 DNS 缺陷,搜集用户信息,通过分析和分类后,给用户发送相关广告[22] .通过跟踪 DNS 流量分析用户行为,这种方法的准确率可达到 88%[23] .这说明攻击者完全可以利用 DNS 查询流量窃取用户隐私.

利用 DNS 漏洞的攻击手段还有很多[24] ,如:1)中间人攻击(MITM),由于 DNS 不提供数据的真实性和完整性校验,解析器无法判断收到数据的真实性和完整性,攻击者可以利用这个漏洞进行中间人攻击,如数据包伪造、事务 ID 欺骗(transaction ID spoofing);2)缓存攻击,使用缓存降低了访问时间,但是会导致数据一致性问题,如攻击者将虚假信息注入到 DNS 缓存中[18] ;3)分布式拒绝服务攻击(DDoS),如对根服务器进行 DDoS 攻击,给全局 DNS 解析带来严重影响.

2.2.2 系统实现脆弱性

DNS 系统的脆弱性源于 DNS 系统的实现、构成和管理方式[15] .互联网中大量开放式 DNS 服务器没有遵守最佳配置原则,也没有进行必要的安全验证,域名解析存在严重的安全隐患.DNS 服务软件也存在大量的漏洞,利用 DNS 服务软件的零日漏洞发起的攻击已是攻击 DNS 的重要手段[10] .

大量的开放式第三方 DNS 服务器管理不规范是 DNS 系统脆弱性的原因之一.DNS 系统经过多年的发展,系统越来越复杂,服务器数目也越来越庞大,其中包含了许多开放的 DNS 服务器.除了熟知的 Google DNS 和 Public DNS 等开放式 DNS 服务器外,仍有大量的由非政府组织和个人等第三方机构架设的开放式 DNS 服务器.但是这些开放式 DNS 服务器存在严重的安全隐患.在域名解析的过程中,可能会涉及不同层级、地域的域名服务器和解析器,但是在数据传输的过程中没有建立安全链接,数据的真实性和完整性也得不到保障.用户的个人信息和浏览记录会泄露给这些开放式 DNS 服务器提供商.

DNS 系统没有遵守最佳配置原则,导致系统存在安全隐患.目前网络上开放式解析器的数目为 $10x10^6$~$32x10^6$ 个[25] ,解析器采用复杂的解析策略,如在树形结构中采用大型共享解析池.这些解析器可以分为 3 类:1)“入口”服务器,负责接收用户的解析请求;2)“出口”服务器,负责与域名服务器交互,返回解析结果:3)中间人服务器,负责转发各种解析请求.其中,后两类解析器对终端用户并不可见.但是这些开放式解析器存在严重的安全隐患,其中只有 19%的解析器能够返回正确的 TTL[26] .此外,网络中存在大量用户无法访问的解析器,这些解析器负责缓存解析结果,提高解析效率.但是这些由第三方机构管理的服务器,在部署和配置管理方面缺乏规范,存在安全隐患[27] .

DNS 实现软件存在漏洞也是系统脆弱性的主要原因.互联网系统协会(Internet Systems Consortium,ISC)调查了 DNS 服务器分布情况[28] ,其中使用数量最多的前 5 个服务器软件如表 2 所示.从表 2 可以发现,BIND 和 Microsoft 服务器软件数量占据了 95%以上.漏洞信息库 CVE 披露[29] ,BIND 软件漏洞高达 102 项,涉及 BIND8、BIND9 和 BIND4.9 等主要的版本,漏洞主要包括 DoS、缓冲区溢出、权限漏洞等.Microsoft 官网发布 DNS 服务器受到缓存嗅探攻击[29] ,除了在配置上进行限制外,没有好的修改办法.Bishop Fox 公司发现 Windows DNS 客户端存在缓存区溢出漏洞[31] ,在 win8/Server 2012 或者更高版本的计算机上,可能会导致恶意 DNS 应答.攻击者利用这个漏洞在应用发送 DNS 请求时可以执行恶意代码.如果攻击者控制了 DNS 服务器(如通过中间人攻击),就可以访问被攻击者的系统.此外,Microsoft DNS 服务器也受到 DoS 攻击[32] ,缓冲区投毒攻击[33] .

Table 2 Domain Server Software Distribution

表 2 域名服务器分布情况

服务器软件	数目	比例
BIND	85615	80.83%
Microsoft	15601	14.73%
TinyDNS	2500	2.36%
simple DNS	797	0.75%
MyDNS	641	0.61%

2.2.3 体系结构脆弱性

DNS 体系结构的脆弱性在于 DNS 根服务器存在单点失效的缺陷,DNS 根服务器的分布也存在严重的失衡,域名检索和控制过于中心化.

DNS 系统虽然采用分层结构设计,但其核心还是由根服务器管理整个 DNS 系统.根服务器负责维护顶级域名(TLD, top level domain)的位置信息,所有的缓存在没有命中的情况下也都是从根服务器开始查询.目前全球共有 13 台根服务器,这 13 台根服务器中有 10 台位于美国、2 台位于英国和瑞典、1 台位于日本. 随着互联网的发展,各国都有在本国设立根服务器的期望,以此加强互联网核心基础设施的参与度,并加强本地 DNS 服务器性能.2015 年 6 月 23 日,基于全新技术架构的全球下一代互联网(IPv6)根服务器测试和运营实验项目——“雪人计划[34] ”发布,该计划在原有 13 台根服务器的基础上,在全球 16 个国家中再配置 25 台 IPv6 根服务器,以期望实现全球互联网的多边共治,但是这只是增加了根服务器的数量,并没有从根本上解决 DNS 体系结构脆弱性问题.

根服务器作为整个 DNS 系统的核心,如果发生单点故障,整个系统将不能正常运行,整个互联网也会受到严重影响.美国东部时间 2002 年 10 月 21 日,13 台根服务器受到有史以来的最严重的也是规模最大的 DDoS 攻击,超过常规 30-40 倍的数据量攻击使其中的 9 台根服务器瘫痪.2007 年 2 月 6 日,DNS 根服务器再次受到 DDoS 攻击,攻击持续近 8 小时,攻击源遍布全球.2012 年 2 月,著名的黑客组织 Anonymous 宣布将会对全球 13 个根服务器进行 DDoS 攻击,通过让根服务器过载瘫痪全球网络.

在域名检索过程中,本地 DNS 服务器没有缓存记录的域名信息都需要访问根服务器,以此获得下一步域名服务器的请求地址.域名验证过程中,部署 DNSSEC 协议的根服务器作为信任锚,存储顶级名称服务器的秘钥和签名记录,为域名验证提供最终的权威认证.根服务器控制域名的解析和验证控制过于集中,这是 DNS 体系结构脆弱性的根本原因.

综合各类 DNS 安全威胁,表 3 总结了 DNS 相关威胁方式和具体攻击实例.

Table 3 DNS security threats and attack instances

表 3 DNS 安全威胁,和攻击实例

安全威胁	攻击方式	形成原因/攻击实例
协议脆弱性	域名欺骗	2014 年 1 月大陆境内顶级域名被重定向到美国 IP 地址 65.49.2.178
	拒绝服务	2016 年 10 月 DNS 服务商受到大规模 DDoS 攻击
系统实现脆弱性	开放式服务器缺陷	开放式 DNS 服务器设计缺陷,配置错误
	软件漏洞	2016 年 9 月 BIND 漏洞使部分 BIND 服务器瘫痪
		Windows DNS 客户端存在缓存区溢出漏洞,缓存中毒
体系结构脆弱性	单点失效	2007 年 2 月 DNS 根服务器遭受大规模 DDoS 攻击 2015 年 11 月 DNS 根服务器遭受大规模 DDoS 攻击

3 DNS 安全增强

针对 DNS 安全威胁的根本原因,本章对近年来在协议、系统、检测监控、体系结构方面的增强方案做了总结和分析.

3.1 协议安全增强

3.1.1 DNSSEC

为了解决 DNS 系统在数据传输过程真实性和完整性保护,IETF(The Internet Engineering Task Force)提出了 DNS 安全增强方案 DNSSEC[35] .DNSSEC 通过对资源记录进行签名,用户在收到相关请求域名信息时也会收到该记录的签名,用户可以根据签名检测数据的真实性和完整性.DNSSEC 在 DNS 的基础上,增加了 4 种安全记录:1)DNSKEY 记录,存储验证 DNS 数据的公钥;2)RRSIG 记录,存储 DNS 资源记录的数字签名;3)DS 记录,用于 DNSKEY 验证,存储密钥标签,加密算法和对应 DNSKEY 的摘要信息;4)NSEC 记录,存储和对应所有者相邻的下一记录,用于否定存在验证.

虽然 DNSSEC 在理论上能够很好地解决虚假域名信息的问题,但是在其实际的部署过程中却没有达到很好的效果.虽然有 89%的顶级域名部署了 DNSSEC,但是二级域名的部署率仅为 3%,.com 域名部署率只有 0.5%[36] .DNSSEC 配置繁琐,每个域将自身的 DS 记录上传到父域并由父域签名,然后在依次上传直至根服务器.客户端可以对每个 DNSSEC 签名的记录构建一条信任链:根域签名顶级域,顶级域签名二级域,依次构建一条信任链.然而仅有大约 1%的.com,.net 和.org 域名部署率 DNSSEC,在这些部署了 DNSSEC 的域名中,有超过 30%的域名由于缺少 DS 记录造成配置错误[36] .

在部署了 DNSSEC 的客户端中,仍有许多客户端出现解析故障.有研究机构对 50 多万个客户端使用 DNSSEC 名字解析情况做了大规模测量,测量结果发现仅小部分的用户受到 DNSSEC 验证保护,DNSSEC 部署会导致端到端解析失败,平均每 10 台部署 DNSSEC 的客户端中,有大约 1 台客户端无法访问域名[37] .此外,DNSSEC 难以解决不同域之间的互操作和信息引用问题[38] .

DNSSEC 使用了公钥密码体系,在加密的过程中也会引入额外的开销.由于 DNSSEC 消息加密开销,大量的 DNS 请求导致服务器频繁计算签名,增加服务器响应时间,大量的包含数字签名的报文也会占据带宽资源[39] .

3.1.2 DNSCurve

为 DNS 系统提供链路层安全保护,DNSCurve[40] 通过椭圆曲线加密算法和密钥分发机制,加密传输过程中的所有 DNS 数据包,提供机密性和完整性保护.DNSCurve 的工作过程如下:1)DNSCurve 服务器首先通过编码机制将公钥嵌入到 NS 资源记录(NS resource record)中,客户端查找 NS 记录,结合预定的编码机制,找到对应的公钥;2)客户端将 DNSCurve 的公钥和一次性随机数(nonce)一起放到密码箱中(cryptographic box),并将这些进行编码后作为扩展 DNSCurve 的查询数据包;3)DNSCurve 名称服务器首先会校验客户端的请求数据包,如果是正确的数据,则将响应数据包通过密码箱进行加密,作为扩展的响应数据包,发送给客户端;否则,DNSCurve 服务器根据请求数据包的出错误原因发送给客户端,客户端收到响应数据包后,进行重新修改或丢弃.虽然 DNSCurve 在 DNS 协议的基础上提供传输过程中的机密性和完整性保护,但是采用 DNSCurve 的递归解析器没办法通知名称服务器关于响应的有效性,因此名称服务器只能盲目信任本地递归解析器.此外,DNSCurve 需要对 DNS 协议进行修改,导致 DNSCurve 的增量部署受到限制[41] .

3.2 系统实现增强

3.2.1 传输协议

当前 DNS 协议使用 UDP 协议传输数据,信息没有进行真实性和完整性验证,因此对 DNS 传输协议进行增强是增强 DNS 安全性的一种手段.T-DNS[42] 使用 TCP 和 TLS 协议替代 UDP 传输 DNS 消息,解析器与服务器首先需要建立 TCP 连接,然后使用 TLS 协议对 DNS 消息的内容进行加密保护,防止内容泄露和恶意篡改.T-DNS 利用 TCP 连接的数量限制机制,能够防止恶意服务器主动推送虚假应答信息,同时使用 TLS 协议保护数据传输安全,解决了数据泄露和恶意篡改问题.这种方式的局限性是建立 TCP 连接会的时间开销会影响解析效率,T-DNS 采用 TCP 和 TLS 协议,与传统的 DNS 不兼容,很难大范围部署.

3.2.2 查询机制

多个 DNS 服务器协同工作,可以在单个服务器解析失败时请求其他服务器,提高系统的健壮性和可用性.多个 DNS 服务器的查询结果进行协商,也会提高域名解析的真实性.

多个 DNS 服务器协同工作,来完成域名解析过程,是提高系统健壮性和可靠性的一种途径.CoDNS[44] 系统采用局部和邻近感知的设计思想来分发 DNS 请求,并实现低延迟、低开销的名称解析.当本地 DNS 服务器失效(丢包、过载或配置错误),CoDNS 自动将请求重定向到健康的协同服务器,有效地减少延迟,提高查询服务的可靠性.虽然协同 DNS 提高了可靠性和性能,但是系统的安全性也会降低,单点失效和故障会很容易传播到整个系统.为了解决这个问题,ConfiDNS 系统[45] 利用多站点协定(multi-site agreement)和每个站点的查询历史,来解决合作查询过程的缺陷.

将多个 DNS 服务器软件查询结果进行对比,以降低 DNS 软件缺陷或漏洞对查询结果准确性的影响.DR-DNS 系统[46] 可以同时运行多个不同的 DNS 服务器软件副本.用户首先将 DNS 请求发送给 DR-DNS,

DR-DNS 将请求分发给不同的 DNS 软件副本,各种 DNS 服务器软件将查询结果返回给 DR-DNS.DR-DNS 使用投票机制,选择出现次数最多的记录,返回给客户端.这种设计的好处是在某种 DNS 软件漏洞攻击和软件缺陷引起的解析错误下,仍然能够对客户端做出正确响应.但是由于投票机制处理开销和不同 DNS 服务器的响应速度问题,DR-DNS 的解析效率较低.

3.2.3 信息保密

当前 DNS 协议并未对传输的信息进行加密和签名,域名查询结果的真实性和隐私性得不到保障,存在查询结果被篡改和隐私泄露的风险[47] .在现有 DNS 系统的基础上,可通过改变 DNS 系统的组织结构和传输协议来提高解析结果的真实性,保护用户隐私.

为了阻止对顶级域名服务器的恶意攻击,OnionDNS[48] 隐藏顶级域名(TLD),并引入了镜像服务器和.o 域作为 OnionDNS 的顶级域,镜像服务器通过 Tor 网络与根服务器管理的.o 域同步更新.镜像服务器位于客户端与根服务器之间,客户端首先通过开放的网络或者 Tor 网络将请求发送到镜像服务器,然后镜像服务器首先查找缓存的.o 域记录,如果有缓存记录,则返回查询结果.如果缓存记录过期或者没有缓存记录,镜像服务器也不会向隐藏的根服务器发起查询请求,防止攻击者将流量注入到 Tor 网络,影响匿名化服务.镜像服务器通过周期性地从隐藏的根服务器获得对应的.o 域的更新记录,并将结果返回给客户端.由于镜像服务器采用 DNSSEC 协议,和隐藏的根服务器通信时真实性可以得到保证.通过这种方式,对匿名的根服务器提供安全保护.为了防止恶意流量注入,镜像服务器在缓存没有命中时也不询问根服务器,而是周期性更新资源记录,会导致解析效率降低.

为了解决第三方 DNS 解析器造成的隐私泄露问题,在传统的 DNS 解析器和 DNS 服务器中引入一个附加的服务器,起到隐私保护的效果.作为一种传统 DNS 替代方案,EncDNS[49] 基于 DNSCurve[40] 协议,在标准的 DNS 消息中封装加密查询内容并在解析器(Conventional Resolver,CR)与 DNS 服务器之间增设 EncDNS 服务器.CR 向 EncDNS 服务器发送解析请求,EncDNS 服务器获得解密后的域名信息,向授权服务器发起查询,然后将查询结果加密封装后,通过 CR 返回给客户端.由于客户端发起的查询信息中,查询内容被加密. CR 不知道查询内容,CR 将查询内容转发给 EncDNS 服务器后,EncDNS 服务器解密得到查询内容,但这条查询请求的 IP 地址是 CR 的地址信息,EncDNS 并不知道具体的用户 IP 地址,因此 EncDNS 和 CR 共同完成解析过程,且不知道用户的完整的请求内容,达到了隐私保护的目的.EncDNS 的局限性在于需要修改 DNS 协议来传输加密的查询信息,不利于广泛部署.

3.3 检测监控

随着互联网的发展,技术在不断进步,攻击手段也在不断变化,仅仅依靠协议的增强和系统的改变不一定能够抵御所有的攻击.因此,在现有系统的基础上,进行有效监控诊断,保护 DNS 系统的正常运行,也是一个重要的安全增强保障.对 DNS 系统进行诊断监控不需要改变现有 DNS 实现方式,具有良好的渐进部署能力,同时能够有效监测各种攻击.检测监控的核心思想是对 DNS 的查询流量进行分析和检测,构造检测系统并运用如机器学习、信息熵等技术对检测结果进行学习和分类,提高检测精度.本节根据检测流量的层级不同分为监测 DNS 用户端与递归服务器间流量和检测 DNS 服务器间流量.

3.3.1 监测 DNS 用户端与递归服务器间流量

BotGAD[53] [54] 通过分析僵尸主机和控制中心、DNS 服务器和其他主机间的流量,以此检测僵尸网络.BotGAD 将组活动映射为向量,计算向量间的相似性,判断组活动中的成员是否参与了恶意活动.映射方法是在每个时间间隔中,生成一组活动,引入一个二元关系表,表的横行表示每个时间间隔,表的列表示组成员的 IP 地址.如果某个时间间隔内,某个组成员的 IP 参与了活动,则此时间间隔和 IP 地址对应的数据为 1,否则为 0,将表的每个列信息提取出来,这列向量就代表每个时间间隔内各 IP 地址参与组活动情况,然后计算向量间的平均相似度,若超过了阈值,则表明组活动参与了僵尸网络的组活动.

Seguio[55] 利用用户端和 ISP 网络的本地 DNS 解析器的通信流量,构建了一种机器—域名的二分图模型,图中的每个节点代表主机和域,边表示主机在观察阶段查询了该域名.每个域节点附有注释,包括 IP 地址、域活动(如第一次被查询的时间).将与已知恶意节点有连接的节点被标记为恶意节点,将属于域名白名单(如根据

alexa.com)的域标记为良性域.对于其中无法标记的未知节点,通过“谁查询了谁”的特证分类,如果一个恶意主机查询了一个未知域,或一个未知主机查询了一个已知的恶意域,则该节点有很大概率为恶意节点.

此外,监测下层 DNS 流量还可以用来检测利用 DNS 流量控制的僵尸网络和 DNS 隧道.对 DNS 流量特征利用聚类算法分类,处于僵尸网络中的节点,在同一类中彼此相似,但与其他类中的节点有着明显的区别,通过这种方式检测僵尸网络的存在[52] [53] .利用 DNS 查询流量中的时间和空间分布关系与信息熵特征结合,也是检测 DNS 流量控制的僵尸网络的一种手段[56] [57] .检测 DNS 隧道目前主要采用 DNS 流量特征匹配、统计分析流量分析的检测技术[58] .

3.3.2 监测 DNS 服务器间流量

根据从多个递归服务器上收集 DNS 的历史信息,Notos[50] 系统利用网络特征、区域特征和黑名单证据特征,来构建一个网络资源合法分配和操作的模型,并运用这些模型为新的域名计算信誉分.如果信誉分过低,则说明这个新的域名参与了恶意活动.

和 Notos 相比,EXPOSURE[51] 不基于历史 DNS 流量,而是检测实时的真实流量信息,并定义了 15 种恶意域名行为特征,并将这些特征分为基于时间、DNS 应答、TTL 值、域名字面信息 4 类,这些特征被存储到特征分类模块中.数据采集模块收集 DNS 数据,特征分类模块将这些数据按照预先设定的 15 个恶意特征进行分类;域名采集模块和数据采集模块同时运行,然后用域名采集模块采集的已知非法与合法域名对分类模块分类后的数据进行标记,对于能够判断合法或非法的域名,则作为训练模块的输入进行训练,分类器模块则根据训练模块的检测模型来判断未标记的数据是合法还是非法.其中分类器模块使用 J48 决策树算法,并应用信息熵的概念使用标记后的数据构造决策树.在本地递归服务器上进行 DNS 流量的检测方案的局限性在于需要在递归服务器上设置大量的数据采集器才能获得一个域的全局信息,但是由于数据的隐私性和采集器部署原因,很难在实际中得到应用.

通过监控高层 DNS 流量来获得 DNS 域的全局视图,以此来检测恶意域名,基于这种思路研究成果有 Kopis[59] .Kopis 与 Notos、EXPOSURE 的明显区别是监控的层级不同,Notos 和 EXPOSURE 监控的是递归服务器,而 Kopis 监控的是顶级名字服务器和授权名字服务器,并通过划分不同的时序监控 DNS 数据.Kopis 有两种操作模式:训练模式和操作模式.训练模式中,训练模块将已知的合法与非法域名集合 KB 在 m 天内的 DNS 数据作为输入,生成特征向量集合 V_{train},每个 KB 中的域名对应 V_{train} 中的一个标签合法或非法,然后使用监督学习技术[60] 构造一个 DNS 合法与非法查询特征的统计分类模型 S,这些查询数据来自于 DNS 的上层流量.在操作模式中,则应用分类模型 S 在某时序内为未知域名设定可信分数,为了给出最终的分数,模型 S 将会计算 m 个连续时序内的平均可信分数,若低于预先设定的阈值 θ,则判断该域名非法.Kopis 的优点是可以独立配置,不需要从其他网络共享数据,从而不必考虑不同组织和区域信息共享的安全和隐私问题.Kopis 的局限性在于对于生存时间较短的域名,如用 DGA 算法生成的域名,检测效率很低.

为了检测 ISP 主干网中威胁用户安全的僵尸网络、钓鱼网站以及垃圾邮件等恶意活动,DAOS[61] 实时检测流经主干网边界的DNS流量,并从域名依赖性和使用位置两个方面的刻画DNS活动特征.其中依赖性从用户角度观察域名的外在使用情况,而位置则关注区域文件中记录的域名内部资源配置,并分别使用有监督的机器学习算法进行检测,然后通过加权平均融合两方面检测结果,及时准确地识别恶意域名.

3.4 体系结构增强

DNS 根服务器作为 DNS 系统的核心,负责 DNS 主目录的维护和管理,这种方式存在单点故障、易受攻击等缺陷.为了解决 DNS 中心化问题,有学者提出设计去中心化的 DNS 系统.DNS 系统去中心后,每个服务器节点都是平等的,单点故障和 DoS 攻击造成的影响将会降低.DNS 的解析过程不再受限于根服务器,不会因为管理等因素对域名进行封锁,也解决根服务器部署数量有限的弊端.

3.4.1 全分布式系统结构

随着 P2P 网络结构的出现,利用 P2P 网络的容错性和负载均衡等特点,有学者提出了基于 P2P 网络的域名解析服务.采用 P2P 结构的域名系统,节点间相互平等,不会发生传统 DNS 服务器单点失败的中心化问题.

建立全分布式 DNS 的一种方案是用分布式哈希表[63] 技术构造一个去中心化的网络,利用分布式哈希表容错和负载均衡的特性实现对现有 DNS 系统的改进,如基于 Chord[68] 的 DDNS[62] 、基于 Kademlia[67] 的 P-DONAS[66] . DDNS 在传统的 DNS 服务器上对资源记录进行查找,DNS 记录的检索和存储通过分布式哈希表来完成.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 $O(logN)$.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 Nodes).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,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 和传统的 DNS 服务器也是兼容的.

为了提高基于分布式哈希表的域名系统的检索效率,基于 Beehive[65] 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[64] 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 采用和传统 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,家节点会和传统的 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 和传统 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公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 高,且查询速率比完全基于 P2P 网络的域名系统快.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有如下的局限性:

- 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的情况下就断开连接,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 由四层组成,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.第一层区块链层,负责存储区块链操作序列,并提供操作写入顺序的共识.第二层是虚拟化层,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.第三层是路由层,Blockstack 从实际的存储数据中分理出路由请求,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.第四层存储层在最顶层,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[78] (Simple Name Verification)协议,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.这四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,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 安全方案做了总结.为了更加直观的分析并对比各种增强方案的优点和局限性做了比较分析.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][82-84].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应计提供技术和框架,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:

(2)高效的 P2 网 P 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[85] .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.

(3)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.

(4)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量盟的方式,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、根联盟同

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,进行放大攻击、投毒攻击等恶意行为.据调查发现,在 3200 万个开放式解析器,其中有 2800 万有严重的安全隐患[83] .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[53-64].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,能够有效监测各种安全威胁.

(2)当前无论是基于机器学习、信息熵、统计分析等理论方法,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的时候及时发现,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 系统广泛应用,有学者虽然提出改进方案,与现有的 DNS 系统不兼容,也很难被大范围部署.DNSSEC 虽然在 1997 年就已经被提出,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%,但是在二级域的部署率仅为 3%[84] .有很多新型的名字服务系统和架构都已提出来[42] [71] [73] ,但是与当前 DNS 系统不兼容,因此这些研究成果很难被网络运营商和大型公司采用.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.针对云环境下 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是值得关注.

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关心的问题.本文对 DNS 安全防护技术进行了全面地分析和总结,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] Leighton, Tom. 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 V A F , Doneda D , Abreu J D S . Cyberwarfare and Digital Governance. IEEE Internet Computing, 2017, 21(2):68-71..

[5] ChineseCN. 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. RFC7626,2015.
[8] FrameworkPOS.https://www.anomali.com/blog/three-month-frameworkpos-malware-campaign-nabs-43000-credits-cards-from-poi
[9] RFC Research. 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. http://www.efficientip.com/resources/white-paper-dns-security-survey-2017/.
[11] AnsteeD, BowenP, ChuiC.F, SockriderG.12th Worldwide Infrastructure Security Report. Arbor Network.2017.
[12] Marc Kührer, Hupperich T , Rossow C , et al. Exit from Hell? Reducing the Impact of Amplification DDoS Attacks. 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 Jian. 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 Qing. The Security of Internet Domain Name System in China. Modern telecommunications technology, 2010, 2010 (4): 9-11 (in Chinese with English abstract)..
[18] Li Jie. Detection of DNS spoofing and cache poisoning attacks (MS. Thesis). 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. The International Conference 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. IETFRFC7626, 2015.
[22] ROSSEBO J, CADZOW S, SIJBEN P, et al. A threat, vulnerability and risk assessment method and tool for Europe. The International Conference 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. Information Security and Privacy Research. Berlin Heidelberg: Springer, 2012:235-248.
[24] S. Ariyapperuma C.J. Mitchell. Security vulnerabilities in DNS and DNSSEC. Availability, Reliability and Security. ARES 2007. The Second International Conference on, 2007, pp. 335-342.
[25] SCHOMP K, CALLAHAN T, RABINOVICH M, et al. On measuring the client-side DNS infrastructure. The Conference on Internet Measurement Conference. 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. 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.
[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.
[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). The 8th ACM conference on Computer and Communications Security, 2001:86-95.
[36] Yang, H., Osterweil, Eric, Massey, Dan, Lu, Songwu, Zhang, Lixia. Deploying Cryptography in Internet-scale Systems: A Case Study on DNSSEC. Dependable and Secure Computing, IEEE Transactions on. 8. 2011:656-669.

[37] Amir Herzberg, Haya Shulman. DNSSEC: Interoperability Challenges and Transition Mechanisms. 2012 Seventh International Conference on Availability, Reliability and Security, 2013:398-405.

[38] HERZBERG A, SHULMAN H. DNSSEC: security and availability challenges. Communications and Network Security, 2013: 365-366.

[39] LIAN W, RESCORLA E, SHACHAM H, et al. Measuring the practical impact of DNSSEC deployment. USENIX Security, 2013:573-588.

[40] Dempsky, M. DNSCurve: Link-Level Security for the Domain Name System. Internet Draft draft-dempsky-dnscurve-01, RFC Editor (2010).

[41] M. Anagnostopoulos, G. Kambourakis, E. Konstantinou, S. Gritzalis. DNSSEC vs. DNSCurve: A Side-by-Side Comparison. IGI Global, 2012:201-220.

[42] ZHU L, HU Z, HEIDEMANN J, et al. Connection-oriented DNS to improve privacy and security. ACM Conference on Sigcomm. 2015:379-380.

[43] Shulman H . Pretty Bad Privacy: Pitfalls of DNS Encryption. Workshop on Privacy in the Electronic Society, 2014:191-200.

[44] Park K, Pai V S, Peterson L, et al. CoDNS: Improving DNS Performance and Reliability via Cooperative Lookups. OSDI Proceedings of the 6th Symposium on Operating Systems Design and Implementation, San Francisco, CA, Dec. 5, 2004: 14-14.

[45] L. Poole and V. S. Pai. ConfiDNS: Leveraging scale and history to improve DNS security. In Proceedings of Third Workshop on Real, Large Distributed Systems (WORLDS), November 2006.

[46] Khurshid A, Kiyak F, Caesar M. Improving Robustness of DNS to Software Vulnerabilities. ACSAC 2011: Proceedings of the 27thAnnual Computer Security Applications Conference, Orlando, Florida, USA, Dec. 5-9, 2011: 177-186.

[47] HUANG Kai, KONG Ning. 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. Communications and Network Security. 2015:379-387

[49] HERRMANN D, FUCHS K, LINDEMANN J, et al. EncDNS: alightweight privacy-preserving name resolution service. Computer Security-ESORICS 2014. 2014:37-55.

[50] ANTONAKAKIS M, PERDISCI R, DAGON D, et al. Building a dynamic reputation system for DNS. Usenix Security. 2010:18-36.

[51] BILGE L, KIRDA E, KRUEGEL C, et al. EXPOSURE: Finding malicious domains using passive DNS analysis. The Network and Distributed System Security Symposium(NDSS 2011). 2011.

[52] Perdisci R, Corona I, Dagon D, Lee W. Detecting malicious flux service networks through passive analysis of recursiveDNS traces. In: Annual computer security applications conference, 2009 (ACSAC'09). IEEE, pp 311–320.

[53] Choi H, Lee H, Kim H. BotGAD: detecting botnets by capturing group activities in network traffic. In: Proceedings of the fourth international ICST conference on communication system softWAre and middlewaRE. ACM, 2009, p 2.

[54] Choi, Hyunsang, and H. Lee. Identifying botnets by capturing group activities in DNS traffic. Computer Networks 56.1, 2012:20-33.

[55] Rahbarinia, Babak, R. Perdisci, and M. Antonakakis. Segugio: Efficient Behavior-Based Tracking of Malware-Control Domains in Large ISP Networks. International Conference on Dependable Systems and Networks IEEE, 2015:403-414.

[56] Huang S-Y, Mao C-H, Lee H-M. Fast-flux service network detection based on spatial snapshot mechanism for delay-free detection. In: Proceedings of the 5th ACM symposium on information, computer and communications security, 2010:101-111.

[57] Yadav S, Reddy AN. Winning with DNS failures: strategies for faster botnet detection. Rajarajan M, Piper F, Wang H, Kesidis G (eds) Security and privacy in communication networks. Springer, Berlin, Heidelberg, 2012:446–459.

[58] DONG Li-peng, CHEN Xing-yuan, YANG Ying-jie, et all. Implementation and Detection of Network Covert Channel. Computer Science,2015,42(07):216-244 (in Chinese with English abstract).

[59] ANTONAKAKIS M, PERDISCI R, LEE W, et al. Detecting malware domains at the upper DNS hierarchy. The 20th USENIX Conference on Security. 2011:21-27.

[60] C. M. Bishop. Pattern Recognition and Machine Learning (Information Science and Statistics). Springer-Verlag New York, Inc., Secaucus, NJ, USA, 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).

[62] Cox R, Muthitacharoen A, Morris R. Serving DNS Using a Peer-to-Peer Lookup Service. IPTPS 2002: Proceedings of the First International Workshop on Peer-to-Peer Systems, Cambridge, MA, USA, March7-8, 2002: 155-165

[63] Frank Dabek, M. Frans Kaashoek, David Karger, Robertn Morris, and Ion Stoica. Wide-area cooperative storage with CFS. ACM Symposium on Operating Systems Principles (SOSP ’01), Chateau Lake Louise, Banff, Canada, October 2001

[64] Ramasubramanian V, Sirer E G u. The Design and Implementation of a Next Generation Name Service for the Internet. SIGCOMM 2004: Proceedings of the 2004 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communications, Aug. 30-Sept. 3, 2004: 331-342.

[65] Ramasubramanian V, Sirer E G u. Beehive: O(1) Lookup Performance for Power-Law Query Distributions in Peer-to-Peer Overlays. NSDI 2004: Proceedings of the 1st Conference on Symposium on Networked Systems Design and Implementation, San Francisco, CA, USA, March 29-31, 2004

[66] Peter Danielis, Vlado Altmann, Jan Skodzik, Tim Wegner. Achim Koerner, and Dirk Timmermann. P-DONAS: A P2P-Based Domain Name System in Access Networks. Acm Transactions on Internet Technology, 2015,15(3) :11

[67] Petar Maymounkov and David Mazières. Kademlia: A Peer-to-Peer Information System Based on the XOR Metric. In Revised Papers from the First International Workshop on Peer-to-Peer Systems (IPTPS '01), Peter Druschel, M. Frans Kaashoek, and Antony I. T. Rowstron (Eds.). Springer-Verlag, London, UK, UK, 2002:53-65.

[68] STOICA I, MORRIS R, KARGER D, et al. Chord: a scalable peer-to-peer lookup service for Internet applications. IEEE/ACM Transactions on Networking, 2003, 11(1): 17-32.

[69] Y. Song and K. Koyanagi. Study on a hybrid P2P based DNS. IEEE International Conference 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).

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

[72] Nakamoto, Satoshi. 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. 2016 USENIX Annual Technical Conference (USENIX ATC 16). 2016: 181-194.

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

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

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

[77] Ittay Eyal and Emin Gun Sirer. Majority is not enough: Bitcoin mining is vulnerable. In Financial Cryptography, 2014.

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

[79] ZHANG Y, XIA C D, FANG B X, et al. An autonomous open root resolution architecture for domain name system in the internet. Journal of Cyber Security, 2017,2 (4)(in Chinese).

[80] Fang Binxing. 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 Guoku, Jiang Wenbao. A Decentralized Domain Name System for the Network. Cyberspace Security,2017,8(01):14-18 (in Chinese with English abstract).

[82] Leslie Lamport.The Part-Time Parliament. ACM Transactions on Computer Systems 16, 2(May 1998),133-169.

[83] Open Resolver Project. http://openresolverproject.org/, May 2016.

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

[85] Lu Z H, Gao X H, Huang S J, et al. Scalable and Reliable Live Streaming Service through Coordinating CDN and P2P. IEEE, International Conference on Parallel and Distributed Systems. IEEE, 2012:581-588.

[86] Bhadauria R, Sanyal S. Survey on security issues in cloud computing and associated mitigation techniques[J]. 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[博士论文].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[硕士论文].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(09):28-36.
[58] 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(07):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.
[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(06):1474-1487.
[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(04):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(01):14-18.