

DNS 安全增强及区块链技术的应用研究进展

倪雪莉^{1,2,3}, 王 群^{1,2+}, 马 卓^{1,2}

1. 江苏警官学院 计算机信息与网络安全系, 南京 210031

2. 江苏省电子数据取证分析工程研究中心, 南京 210031

3. 南京信息工程大学 计算机学院、网络空间安全学院, 南京 210044

+ 通信作者 E-mail: wqun@jspi.edu.cn

摘 要: 因设计之初对安全性考虑的缺失, 致使当今的 DNS 面临日益复杂和极具挑战性的安全问题, 而区块链技术的应用, 以其独有的去中心化、防篡改、可溯源、公开透明等特征, 为解决当前 DNS 面临的安全威胁提供了一种崭新的思路。在系统分析 DNS 脆弱性和安全威胁的基础上, 对 DNS 安全增强技术进行了系统梳理与剖析, 强调了区块链在增强 DNS 系统安全性以及重构 DNS 安全体系中发挥的独特功能和技术优势。概述了 DNS 的工作机制, 分析了 DNS 安全脆弱性的具体表现和产生根源, 总结了典型 DNS 攻击方式与检测方法; 围绕体系结构、协议和实现过程三个维度分别对传统 DNS 安全增强技术的研究成果进行了对比分析; 将区块链在 DNS 安全防护中的应用界定为融入区块链的 DNS 安全增强技术和基于区块链的 DNS 安全方案两种类型, 以代表性示例分别分析了各区块链安全方案的实现方法和技术路径, 并进行了分析与比较; 总结并提出了区块链 DNS 目前仍然存在的去中心化与效率、不可篡改与合规、安全与用户体验等悬而未决的问题, 且对 DNS 安全增强未来可能的研究热点和方向进行了展望。

关键词: DNS 安全; DNS 脆弱性; 区块链技术; DNS 安全增强

文献标志码: A **中图分类号:** TP393

Research Progress on Blockchain-Based DNS Security Enhancement Technology

NI Xueli^{1,2,3}, WANG Qun^{1,2+}, MA Zhuo^{1,2}

1. Department of Computer Information and Cybersecurity, Jiangsu Police Institute, Nanjing 210031, China

2. Jiangsu Electronic Data Forensics and Analysis Engineering Research Center, Nanjing 210031, China

3. School of Computer Science, School of Cyber Science and Engineering, Nanjing University of Information Science and Technology, Nanjing 210044, China

Abstract: Due to insufficient security considerations in its initial design, the domain name system (DNS) now faces increasingly complex and challenging security threats. Blockchain technology, with its unique characteristics of decentralization, tamper-resistance, traceability and transparency, provides a novel approach to addressing these security threats. Based on the systematic analysis of DNS vulnerabilities and security threats, this paper summarizes existing DNS security enhancement technologies, and emphasizes the unique functional and technical advantages of blockchain in improving DNS security and reconstructing its security framework. Firstly, this paper provides an overview of the working mecha-

基金项目: 国家自然科学基金(61802155, 62202209); 江苏省高校优秀科技创新团队项目; 公安技术、网络空间安全“十四五”江苏省重点学科; 公安部科技计划项目(2023JSZ09); 教育部人文社会科学研究规划基金(24YJAZH158)。

This work was supported by the National Natural Science Foundation of China (61802155, 62202209), the Project of Excellent Scientific and Technological Innovation Team of Jiangsu Universities, the Key Disciplines of Jiangsu Province in the 14th Five-Year Plan: Public Security Technology and Cyberspace Security, the Science and Technology Project of Ministry of Public Security of China (2023JSZ09), and the Humanity and Social Science Planning Foundation of Ministry of Education of China (24YJAZH158).

收稿日期: 2025-04-07 **修回日期:** 2025-06-03

nism of DNS, analyzes the specific manifestations and root causes of DNS vulnerability, and summarizes typical DNS attack methods and detection techniques. Secondly, the research results of traditional DNS security enhancement technologies are systematically summarized from three aspects: architecture, protocol and implementation process. Thirdly, the application of blockchain in DNS security protection is divided into two types: DNS security enhancement technologies integrated with blockchain and blockchain based DNS security solutions, and their implementation methods and technical paths are detailed with representative examples. Finally, this paper points out the unresolved issues of blockchain DNS, such as the trade-off between decentralization and efficiency, the conflict between immutability and compliance, and the balance between security and user experience, and prospects for the possible future research hotspots and directions of DNS security enhancement.

Key words: DNS security; DNS vulnerability; blockchain technology; DNS security enhancement

作为互联网神经中枢的域名系统(domain name system, DNS)的核心功能是建立域名和IP(Internet protocol)地址两类网络标识体系之间的相互转换机制,但其存在的安全问题长期以来备受社会各界的诟病,也是一个尚未摆脱的困扰。安全与应用相伴而生,迭代发展。自从1983年由Mockapetris^[1]首次提出DNS以来,根据互联网的应用和技术演进,本文将DNS的发展划分为以下三个阶段:(1)单一的“查询/响应”系统。这是DNS发展的起步阶段,域名拥有者一般会在本地网络中独立搭建DNS解析服务器,以“查询/响应”方式提供域名与IP地址间的解析服务。在这一阶段,DNS安全威胁主要来自于DNS协议本身以及DNS解析服务器软件存在的安全漏洞。主要攻击方式有针对DNS协议的中间人(man in the middle, MITM)攻击^[2]、分布式拒绝服务(distributed denial of service, DDoS)攻击^[3]、利用DNS服务软件(如BIND、NSD(name server daemon)、Knot等)漏洞的攻击^[4]等。针对这些攻击方式的典型防御机制是DNS安全扩展(domain name system security extensions, DNSSEC)^[5]。(2)智能流量调度平台。移动互联网的兴起催生了新的应用业态,也对DNS的功能提出了挑战,原有自行部署、功能单一的DNS解析服务已无法满足智能手机、物联网终端等移动应用的需求,亟需性能更加强大的可信第三方公共域名解析服务平台的支撑,典型代表有Google公司的8.8.8.8和Cloudflare公司的1.1.1.1。在该阶段,DNS已经蜕变为一个基于名称解析服务的智能流量访问控制和调度系统,DNS除提供域名与IP地址之间的静态映射关系外,已经发展为一种面向业务应用的服务平台,具有流量监测、访问控制、用户位置感知等丰富功能。这时的DNS面对的最大安全隐患是平台的安全性、可信性和可扩展性,DNS的服务更加集中,任何一次故障产生的影响力更大、影响范围更广。在这一阶段,典型的DNS安全威胁有DDoS攻击、DNS反射放大攻击^[6]以及利用平台系统漏洞发起的

各类针对DNS的攻击^[7-8]等,主要防御手段则是针对系统漏洞的DNS攻击检测技术^[9-10]。(3)云解析DNS平台。随着以云计算、工业互联网、人工智能等为代表的新基建的飞速发展,传统DNS解析技术在应对高流量、高并发等复杂极端场景时显得无能为力,云解析DNS^[11]以其具有的智能、安全、高效等特征成为新一代DNS解析技术而备受关注。云解析DNS基于云技术,可在全网范围内根据流量要求设置DNS解析服务节点,并通过智能调度算法将用户的域名解析请求转发给就近的解析节点,从而提升DNS解析效能,提高DNS解析服务的稳定性和高可用性。由于云解析DNS一般内置了DDoS防火墙、DNSSEC、流量清洗等安全机制,能够有效抵御DNS劫持、缓存区中毒等安全威胁,而且部署灵活,提供了负载均衡、冗余备份、智能解析等功能,以满足不同场景下的应用需求。诚然,云计算中存在的云虚拟化安全、云硬件安全、云数据安全、云应用安全等安全问题,同样会对云解析DNS构成安全威胁^[12],结合DNS运行机制来加强云计算安全研究是提升DNS安全性有效途径。

以上分析不难看出,伴随着DNS作为国家信息基础设施重要性的不断提升,其安全性也变得更加重要。因此,在系统梳理DNS安全风险的基础上加强对其安全增强技术的研究显得极其重要和必要。近年来,国内外研究者针对DNS安全问题提出了一些卓有成效的应对策略和新颖的解决思路。在国外研究方面,Schmid^[13]认为DNS在设计之初强调了速度、可扩展性和可靠性,而忽视了安全性和隐私性。在此情况下,虽然DNSSEC等安全机制被广泛采用,但DNS攻击正变得越来越频繁、复杂和危险。Lyu等人^[14]通过对2016年至2021年间发表的DNS加密文献的整理,分析了已有标准和技术存在的不足,为提高DNS加密的性能和安全性提出了几个研究方向。Al-Mashhadi等人^[15]认为基于区块链的DNS在设计上是安全的,同时指出只有完全解决区块

链目前面临的主要挑战,才能用其替代现有的 DNS。在国内研究方面,王文通等人^[16]对 DNS 安全的脆弱性及其增强技术进行了综述;张宾等人^[17]从直接面向用户的递归解析服务器(recursive server)出发,全面梳理和总结了 DNS 存在的安全威胁和相应的安全防护技术;夏玲玲等人^[18]对区块链在公钥密钥基础设施(public key infrastructure, PKI)安全中的应用进行了系统研究,而 PKI 是构建安全 DNS 的基础。以上研究虽各有侧重,但均缺乏对 DNS 安全描述的完整性和系统性,并未形成从知识背景到安全分析、再到防御机制的完整论述,更没有形成有说服力的比较结果,未证明区块链在 DNS 安全增强技术中的应用优势。为此,本文以背景知识、问题剖析与解决、分析比较以及未来展望为主线,在系统探讨 DNS 工作机理及存在的安全风险的基础上,阐述主要的 DNS 安全增强技术,并突出区块链发挥的应用优势和发展趋势。本文的主要贡献为:一是将 DNS 发展归纳为 3 个阶段,在此基础上系统分析了 DNS 的脆弱性和攻击与检测方式;二是提出基于“体系结构+协议+实现”研究架构,使得对 DNS 安全增强的研究更具系统性和针对性;三是创新性地将区块链在 DNS 安全防护中的应用界定为融入区块链的 DNS 安全增强技术和基于区块链的 DNS 安全方案两种类型,并以代表性示例分别对比分析其实现方法和技术路径;四是紧密结合区块链特征及技术优势,提出了目前区块链 DNS 仍然存在的一些悬而未决的问题,并指出了 DNS 安全增强未来可能的研究热点和方向。

1 背景知识

1.1 DNS 的工作机制

DNS 的主要工作过程是:主机中的存根解析器(stub resolver)通过调用 gethostbyname 或相关进程,向本地递归解析服务器发送一个查询请求,本地递归解析服务器在收到该查询请求后将向一组权威名字服务器(authoritative name server)发起迭代查询,并将查询结果返回给主机。DNS 主要由域名空间及资源记录、名字服务器、解析器 3 部分组成,如图 1 所示^[19]。其中:

(1)域名空间及资源记录。域名体系采用层次树形结构组织 DNS 域名空间。资源记录包含了所有的 DNS 请求和响应信息,每条资源记录是一个由 Domain_name(域名)、Time_to_live(生存期)、Class(类别)、Type(类型)和 Value(值)组成的五元组,存放在域名空间的各域名服务器中。Internet 的域名空间由 Internet 名称与号码分配机构(Internet corporation for assigned names and numbers, ICANN)统一管理。目前全球有 13 台根服务

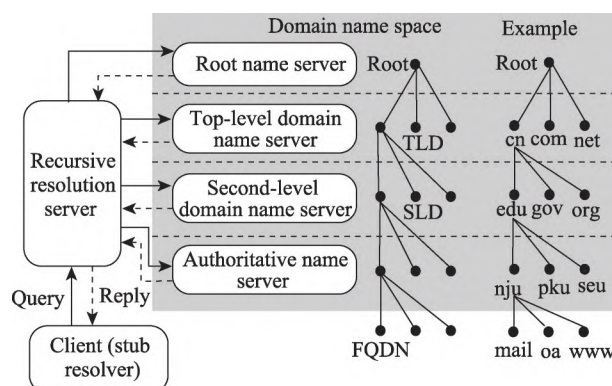


图1 DNS体系结构

Fig.1 Architecture of DNS

器,其下的顶级域(top level domain, TLD)通常包括按行业领域不同而创建的通用顶级域(generic TLD, gTLD,如表示商业的.com、教育科研的.edu、政府的.gov等)以及代表国家或地区的国家代码顶级域(country code TLD, ccTLD,如代表中国的.cn、代表美国的.us等)。域名注册机构向TLD申请获得代表特定组织的二级域(second level domain, SLD),然后向各个组织或用户提供基于SLD的子域注册。拥有合法子域的用户可以根据资源管理需要自行创建称为叶子节点的完全限定域名(fully qualified domain name, FQDN)。需要说明的是,ICANN的功能最初由互联网号码分配局(Internet assigned numbers authority, IANA)及其他一些组织负责,为便于说明,本文全部使用ICANN。

(2)名字服务器。名字服务器具体负责域名与IP地址之间的转换,可分为连接用户端和权威服务器端的本地递归解析服务器,以及保存DNS树形结构和相关配置信息的权威名字服务器。权威名字服务器从最顶层的根域名服务器到最下层的权威域名服务器,分别提供针对域名空间的权威解析,同时以区域(zone)文件来管理与域名相关的资源记录信息。出于安全考虑,一个针对特定域名服务的名字服务器一般由一台主名字服务器和多台辅助域名服务器组成,辅助域名服务器通过区域传输(zone transfer)从主名字服务器获取区域文件的副本,从而实现资源记录信息的同步。另外,在DNS系统中还存在一些专门提供域名解析结果缓存功能的DNS缓存服务器以及只负责域名转发的域名转发服务器等^[20]。

(3)解析器。解析器(resolver)的核心功能是响应查询请求,将从域名空间中获得的查询结果返回给DNS查询端。当主机中的解析器收到一个域名查询请求时,首先在本地缓存中进行查询,在本地查询未果的情况下将向在主机中配置的递归解析服务器继续发起

查询请求。递归解析服务器在接收到查询请求后,首先在其资源记录中查找是否存在对应的权威源,如果存在则返回权威查询结果,否则将从缓存中查询,当缓存中仍然未发现时将进入迭代查询过程。由于每个递归服务器上都保存有一个包含所有根服务器的名字与对应IP地址的根区提示文件(hint file),递归解析服务器在本地查询未果的情况下,将向根域名服务器发起迭代查询,然后依次与顶级域名服务器、二级域名服务器和权威域名服务器之间进行查询/应答交互,最后主机得到域名对应的IP地址。在此过程中,所有发出请求的域名服务器都会缓存应答结果,通常情况下,递归解析服务器会缓存80%以上的域名解析结果,只有不到20%的查询请求需要进入迭代查询阶段。

1.2 DNS脆弱性分析

遵循“体系结构+协议+实现”的研究思路,本文将DNS存在的脆弱性分为体系结构的脆弱性、协议的脆弱性和实现过程的脆弱性3部分。

1.2.1 体系结构的脆弱性分析

DNS体系结构采用树形分层模型,其中管理整个DNS系统且负责维护TLD位置信息的根服务器位于最顶端,当DNS查询在所有缓存中未获得有效响应时,将从根服务器开始进入迭代查询阶段。因此,根服务器在域名空间中具有绝对的权威性,对域名查询提供初始的权威资源记录。

根服务器管理采用的完全中心化方式是影响DNS安全的主要原因。ICANN作为根服务器唯一的权威管理机构,统一管理着所有的根服务器列表,托管在不同机构的根服务器使用的根区(root zone)全部由ICANN指定,实现了根服务器日常运维与根区管理的分离。在此模式下,所有的TLD都需要ICANN的授权,但TLD的管理权力归属于相关机构(如gTLD)或国家(如ccTLD)^[21],即TLD服务器存在权力与管理的相互分离。完全中心化的管理机制下,根服务器对TLD具有绝对控制权,可以通过篡改根区文件中的TLD授权信息来破坏顶级域名服务器的正常解析功能,或通过直接删除根区文件中的TLD授权信息使特定的TLD在互联网域名空间中消失。

目前,全球共有13个根服务器^[22],其中仅有的1个主根服务器在美国,由美国互联网机构Network Solutions运维,其余12个辅根服务器中有9个在美国,2个在欧洲(分别位于英国和瑞典),1个位于日本,这13个根服务器分别由12个独立的机构单独管理(其中VeriSign公司同时管理了2个)。在DNS所使用的用户数据报协议(user datagram protocol,UDP)报文中,13个根服务器分

别用字母A~M标识。对于缺乏根服务器的国家或地区,只有通过根服务器的镜像来优化本国或本地区的DNS解析。中国自2003年引进第一个根服务器(F根服务器)的镜像以来,相继又引进了I、J、L等根服务器的镜像节点,为中国境内的DNS解析提供了根节点服务。由于域名空间中根服务器功能的极端重要性以及地理分布的特殊性,在外因(如政治因素)影响或人为配置失误时,从根区文件中删除或篡改特定的TLD授权信息是完全可能的,因为TLD授权信息由其权威机构提交给ICANN后,由ICANN负责将修改后的根区文件内容向所有的根服务器定向传播,TLD权威机构无权对根区文件进行管控。因此,在域名查询过程中,当递归解析服务器中找不到所查询域名的资源记录时就需要从根服务器开始进行迭代查询,而DNS根服务器存在严重的单点故障和单点失效风险,这就是DNS体系结构存在脆弱性的根本原因。

1.2.2 协议的脆弱性

DNS协议在设计之初强调了功能实现,而忽视了安全防御,由此导致的协议脆弱性主要表现在以下几个方面:

(1)采用UDP协议传输DNS报文。DNS的查询和应答报文均采用UDP协议以明文方式传输,其中报文中承载的数据未进行加密处理,资源记录也没有提供签名验证机制以防止被伪造,因此网络中传输的DNS信息容易遭受窃听、篡改和伪造等攻击。同时,根据DNS报文中不同字段的功能定义,攻击者可以通过篡改相应的字段信息实施中间人攻击,例如通过篡改报文中的“事务ID”字段,让查询报文无法得到正确的应答报文等。

(2)使用未加密的缓存架构。在DNS系统中,发出查询请求的服务器都会在其缓存中保存相应的应答信息,以备在后续查询中给以快速响应。但是,以明文方式保存在缓存中的数据易遭受缓存区中毒攻击^[23]。由于互联网的开放性,大量未受任何安全防护的开放解析器(尤其是组织自行架设和免费使用的DNS解析器)成为攻击者的目标,通过注入攻击来篡改缓存中的数据,进而破坏DNS数据的真实性与完整性。

(3)存在隐私泄露风险^[24-25]。DNS查询报文携带了大量的隐私信息,其中包括查询用户的兴趣爱好、位置信息、设备类型以及用户真实姓名等内容。例如,当用户利用浏览器访问某些站点时会触发DNS主动查询过程,此过程可能会泄露用户的上网习惯以及对特定内容或站点访问的偏好,即使是在用户没有察觉的情况下从后台发生的被动查询,也会通过流量分析窥探出用户的隐私。一些非法组织通过搜集并分析用户DNS信息,

对用户进行精准画像和商业行为设计,剖析用户真实网络行为,明确人群划分,推送相关广告等。另外,随着物联网应用的不断普及,DNS 查询数据可能会暴露智能终端制造商、型号特征以及设备漏洞等信息,DNS 已经成为互联网中泄露隐私最严重的领域^[26]。

1.2.3 实现过程的脆弱性

DNS 系统的脆弱性相当部分来自于实现过程,主要体现在 DNS 服务的开放性和软件漏洞 2 个方面。

(1)DNS 服务器的开放性。DNS 从一个简单的域名查询数据库发展成为今天的一个分布式智能算力和流量调度平台,在其功能和应用场景变得愈加丰富的同时,其流量的集中化和平台化现象也更加严重。然而,大量的 DNS 服务器尤其是为用户提供直接服务的递归解析服务器在部署和管理上缺乏规范性和约束性,互联网上大量开放的 DNS 服务器成为隐私泄露和网络攻击的源头。大量开放或免费的位于 DNS 体系不同层级的名字服务器和递归解析服务器,在未得到有效监管的情况下,不但数据的真实性和完整性无法得到保障,平台所有者还可能会非法搜集用户的隐私数据并成为网络黑灰产的信息源。另外,由于 DNS 系统的多层树形结构在设计之初并没有对节点采用签名验证机制,同时大量解析器在部署时没有设置准入机制,致使 DNS 服务器之间缺乏安全链接,存在安全隐患。尤其,当 DNS 解析服务器从单一设备发展到云平台时,如何确保 DNS 区域文件和 DNS 托管服务的稳定性和高可用性仍然存在较大挑战。

(2)软件漏洞。与互联网中的大部分应用系统一

样,设计 DNS 系统时无法穷尽所有的逻辑组合,必然产生因逻辑上存在的不严谨而导致的缺陷,利用 DNS 软件存在的缺陷进行漏洞挖掘成为目前网络攻击的主要手段。DNS 软件是部署在通用操作系统上的可独立运行的一类网络协议软件。由于该类软件在运行时需要对外开放相应接口,并进行复杂的协议交互,其漏洞的成因远比通用软件更加隐蔽且难以检测,危害性也更大。目前,互联网中使用较为广泛的 DNS 服务器软件有 BIND、Microsoft DNS Server、TinyDNS、simple DNS、MyDNS 等。其中开源软件 BIND 在所有 DNS 软件中的占比超过了 80%^[27],其存在的漏洞虽然在版本迭代中不断得到修复,但因漏洞未及时发现或修复而引起的网络攻击现象时有发生。BIND 软件存在的典型安全漏洞有安全绕过漏洞、远程利用漏洞、缓冲区溢出漏洞等,利用这些漏洞可以实现对 DNS 服务、数据及平台的攻击。另外,一些开源 DNS 服务器软件由于软件代码的透明性,攻击者更容易挖掘出存在的漏洞并有针对性地构建攻击场景。同时,部分开源社区并不会严格遵守协同漏洞披露(coordinated vulnerability disclosure,CVD)政策,部分发现的漏洞未及时披露和发布补丁,被泄露的漏洞信息可能会被攻击者利用实施零日(zero day,0day)攻击^[28]。还有,DNS 系统的实现除 DNS 服务器软件外,还需要通用操作系统及相关组件的支持,这些软件自身存在的安全漏洞也是威胁 DNS 系统安全的重要因素。

表 1 是互联网域名系统国家工程研究中心对 2024 年 1 至 9 月间发生的 DNS 重要安全事件总结的部分信息^[29]。从中可以看出,这些安全事件不仅针对 DNS 系

表 1 2024 年 1 至 9 月全球 DNS 重要安全事件汇总

Table 1 Summary of global DNS significant security events from January to September 2024

时间	攻击方式	攻击对象	攻击现象及结果描述
2024 年 2 月	DoS	全球互联网	攻击者利用隐藏在 DNSSEC 中的 KeyTrap 存在的严重漏洞发起 DoS 攻击,长时间阻断应用程序访问互联网
2024 年 2 月	域名劫持	知名品牌的域名和子域名	控制了全球 8 000 多个合法互联网域名和 1.3 万个子域名,利用知名品牌(如 MSN、VMware、McAfee 等)的合法域名来绕过垃圾邮件过滤器,每天发送 500 多万封用于诈骗和恶意广告盈利的垃圾邮件子邮件
2024 年 5 月	木马植入	部分印度政府网站	部分印度政府的“gov.in”网站被黑客植入木马程序,将访问者重定向到指定的在线博彩平台,声称可以进行游戏投注
2024 年 5 月	DoS	DNS 系统	使用被命名为“DNSBomb”的工具,将包括超时(timeout)、查询聚合(query aggregation)和快速返回响应(fast-returning response)等常见的 DNS 机制巧妙设计成恶意攻击工具,在短时间内将大量 DNS 响应汇集成为高频次周期性 DNS 脉冲攻击
2024 年 7 月	域名劫持	Squarespace 平台	攻击者利用托管在 Squarespace 平台上的 120 多个 DeFi 应用存在的安全漏洞,通过域名劫持,将用户对 DeFi 应用的访问重定向到钓鱼网站后窃取敏感信息和资金
2024 年 8 月	篡改 DNS 解析信息	家用路由器	攻击者通过搜集公网可访问的路由器地址,利用发现的漏洞或弱口令获取路由器控制权限,然后修改路由器 DNS 服务器地址,达到中间人攻击的效果
2024 年 9 月	CNAME 记录被滥用	合法投资者	网络犯罪组织 Savvy Seahorse 通过滥用 DNS 中的 CNAME 记录来创建支持金融欺诈活动的流量分发系统(traffic distribution systems,TDS),再通过 Facebook 广告将受害者诱导至虚假投资平台,诱骗受害者存入资金并输入敏感个人信息

统,还有利用DNS资源记录对其他网络基础设施发起的攻击。攻击对象既包括全球互联网基础设施,也包括部分国家的政府网站和知名企业的信息系统,甚至是一些国家的家用网络终端,攻击造成的安全事件的涉及面大到全球范围,小到家庭用户。另外,2025年1月,某境外组织通过入侵国内某能源企业路由器,通过植入恶意代码篡改DNS配置,并利用加密隧道与境外C2服务器(command and control server)通信,意图引发区域性停电;2025年5月12日,全球知名的去中心化交易所Curve Finance的DNS遭黑客二次劫持攻击,用户访问被导向恶意网站。

1.3 典型的DNS攻击方式与检测方法

受DNS脆弱性影响,针对DNS协议、体系结构和实现过程漏洞的各类攻击行为频繁发生,成为威胁DNS系统安全的主要因素。表2汇总了典型攻击方法的实现机理以及攻击可能产生的结果,同时有针对性地提供了相应的检测方法。需要说明的是,作为资源记录的存储平台,区块链为攻击检测手段提供了可信验证的数据源,并未提供直接的检测手段。

2 传统DNS增强技术

在前文针对DNS脆弱性分析的基础上,本章遵循对计算机网络的研究思路,仍然从体系结构、协议和实现过程3个方面分别讨论传统DNS增强技术。

2.1 体系结构增强技术

体系结构是安全的基础,一旦确定就难以在现有环境中改变,一般只能借助已有技术来加固。DNS体系结构的脆弱性源于中心化部署存在的单点故障(易遭受DoS/DDoS攻击),以及因软件或系统参数错误配置带来的运行风险。在引入区块链技术之前,传统从体系结构出发解决DNS安全问题的方式是利用分布式系统来改造中心化部署,从体系结构上增强DNS系统的安全性。

2.1.1 DNS根服务器扩展

根区文件管理是加强DNS根服务器安全稳定的关键。根服务器是DNS解析的源头,DNS根服务器的架构应保持相对的稳定。然而,随着互联网承载业务的不断增加,DNS根服务器也在不断演进中担负着更多的功能。为此,DNS根服务器需要在确保安全稳定前的

表2 典型的DNS攻击方式及其检测方法汇总

Table 2 Summary of typical DNS attack modes and detection methods

攻击方式	主要安全威胁	威胁程度	攻击机理	攻击结果	主要检测方法
DoS/DDoS ^[3]	协议脆弱性/实现过程脆弱性	高	通过控制大量傀儡机生成的巨大流量耗尽被攻击对象的资源	被攻击的DNS服务节点失去服务能力	离线或在线检测技术 ^[30-31]
DNS欺骗 ^[32]	协议脆弱性	高	对用户的DNS查询抢先应答(典型场景为MITM)	恶意的DNS流量劫持或善意的DNS流量拦截	主动测量技术 ^[33]
DNS重绑定(rebinding) ^[34]	协议脆弱性	高	利用DNS协议漏洞构建响应报文和恶意HTML文档,欺骗被攻击的受防火墙保护的服务器	绕过边界安全防火墙,渗透到位于防火墙后端的内部服务器后窃取信息	Web浏览器检测和安全隐患阻断技术 ^[34]
DNS劫持 ^[35]	协议脆弱性	较高	将用户正常的Web浏览劫持到特定网页或在APP中嵌入弹窗	用户无法正常浏览网站信息或通过网络钓鱼来窃密	流量检测和特征提取 ^[36]
缓存区中毒 ^[37]	协议脆弱性	高	用虚假IP地址替换掉DNS缓存中的地址并缓存记录	实现域名劫持,进一步实施网络钓鱼、植入木马等攻击	实时监测缓存区中的记录信息
反射放大攻击 ^[6]	体系结构脆弱性	较高	利用DNS应答报文大于查询报文的特征来放大攻击流量	利用被放大几十倍的攻击流量消耗被攻击主机的资源,直至瘫痪	过滤伪造源IP地址的DNS查询 ^[38]
僵尸网络(Botnet) ^[39]	体系结构脆弱性	中	控制者通过命令与控制(command and control, C&C)服务器,利用DNS服务实施攻击	攻击者通过僵尸网络进行垃圾邮件、信息窃取、行网络欺诈、DDoS等攻击	恶意域名和IP地址检测 ^[40]
DGA ^[41]	体系结构脆弱性	较高	利用域名生成算法(domain generation algorithm, DGA)生成大量的虚拟域名实施恶意攻击	在互联网中存在大量恶意域名,破坏域名系统的安全性和可信性	恶意域名和IP地址检测
隐蔽信道 ^[42]	体系结构脆弱性	较高	将与DNS协议无关的内容封装在DNS报文中,然后以DNS协议方式传输	攻击者绕过防火墙等安全设施实现与内部主机之间的隐蔽通信(如文件传输、远程控制等)	特征提取与分析,基于规则及模型的检测 ^[42]
软件漏洞 ^[43-44]	实现过程脆弱性	高	开发DNS系统时因疏忽或编程语言的局限性而存在的安全隐患或局限性	DNS系统执行错误或出现安全问题	网络协议漏洞挖掘 ^[45]
配置错误 ^[46]	实现过程脆弱性	较高	由不同组织管理的区域(zone)文件在配置过程中出现错误	DNS服务器出现解析错误,或出现不存在的域名服务等	DNS检测工具 ^[47] 或数学模型 ^[48]

提下进行渐进式的扩展。

为了有序稳妥地推进 DNS 服务器的扩展工作, ICANN 和相关组织的工作人员成立了根扩展工作组 (root scaling steering group, RSSG) 来确定制定具体工作方案和规范, 并于 2009 年发布了 2 篇研究报告^[49-50]。报告指出, 由于根区文件包含的信息量越来越大, 在网络质量较差的区域, 根区文件的频繁更新将导致根服务的不稳定。目前, 由 VeriSign 公司具体负责根区文件的更新工作, 每天随机更新 2 次, 具体操作流程如图 2 所示^[50]: 当需要进行根区文件更新时, 由全网唯一的称为隐藏根的分发主服务器 (distribution masters, DM) 向其他所有根服务器 (root server, RS) 发送一个 DNS 通告 (notify) 消息, 接收到 DNS 通告消息的每个 RS 都需要回复一个 DNS 通告确认 (acknowledgement) 消息; 如果 DM 在设置时间内没有收到某个 RS 的通告确认消息时将再次发送通告消息, 以便顺利完成根区文件的更新; 当 RS 发送了通告确认信息后, 相继发送一个起始授权管理 (start of administration, SOA) 消息, 告诉 DM 自己当前根区文件的版本号; 当 DM 发现自己的根区文件版本号新于 RS 端时, 则告知 RS 端启动区传输 (zone transfer, XFR), RS 开始区文件的更新操作。另外, 对于根服务器与镜像服务器之间的区文件更新通常采用任播 (anycast) 技术进行。

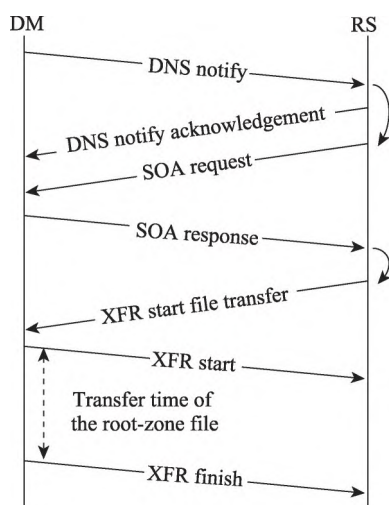


图2 DNS 根区文件的更新过程

Fig.2 Update process of DNS root zone file

借鉴互联网发展中取得的成功经验, DNS 系统尤其是根服务器的扩展可以遵循去中心化和本地化部署。其中, 去中心化是指将当前由有限数量的几个公司承担的对根服务器的相关审核和监管职责由去中心化机制替代; 本地化部署是指在目前 13 个根服务器的基

础上通过增加根服务器的数量来满足本地化需求, 不再受目前根服务器集中化部署和根镜像服务器存在的种种限制。

通常情况下, DNS 采用 UDP 协议传输, 而互联网环境中 UDP 报文长度被限制在 512 Byte 之内, 这也是当时创建根服务器时节点被确定为 13 的主要原因。随着 IPv6 在全球的普及, 根服务器相应的需要兼容 IPv6, 这将导致 DNS 报文长度超过 512 Byte。在此情况下, 存在两种有效的解决途径: 一是 DNS 报文长度突破 512 Byte 限制^[51]; 二是使用 TCP (transmission control protocol) 协议来传输 DNS 报文^[52]。目前, 互联网中路由器的最大传输单位 (maximum transmission unit, MTU) 普遍支持超过 512 Byte 的 UDP 报文, 而且用户与递归服务器之间也允许使用大于 512 Byte 的 DNS 报文进行域名解析, DNS 报文长度突破 512 Byte 限制目前已经不是问题。同时, 由于一个 TCP 报文的最大值 65 535 Byte, 当 DNS 采用 TCP 查询时, 根服务器的配置将不需要考虑报文长度的影响。目前广泛使用的 DNS 递归服务器软件 BIND 从 v9 版本开始就支持 EDNS0 (extension mechanisms for DNS version 0)^[53] 协议扩展机制。该机制在遵循已有 DNS 报文格式不变的基础上, 通过引入一种新的不被缓存、不能被转发且不能被存储在 zone 文件中资源记录 (resource record, RR) 来保持向后兼容性 (backward compatibility), 通过动态探测递归解析服务器与权威名字服务器之间可支持的 UDP 报文大小来协商具体的值, 支持 DNSSEC 协议的 DNS 服务器同时也支持 EDNS0。

2.1.2 利用 P2P 网络的分布式部署

点对点 (peer-to-peer, P2P) 网络^[54] 是构建在互联网之上的一种使用非常广泛的覆盖网络, 具有典型的高度自治和去中心化特征, 是在数据平面构建 DNS 体系, 实现域名资源记录存储和查询的有效手段。利用 P2P 网络部署的 DNS 系统主要包括以下几个方面:

(1) DDNS^[55]

分布式哈希表 (distributed hash table, DHT)^[56] 是构建去中心化 P2P 网络的一种典型技术, 可利用其具有的系统容错和负载均衡特征来改进现有 DNS 系统, 以分布式机制解决当前根服务存在的安全问题。DDNS 使用了可实现对海量数据进行存储和快速查询的 DHash (difference hash) 项目^[57], 实现对 DNS 记录的存储、服务、复制和缓存。DHash 采用类似 Chord^[58] 的环形结构, 充分发挥了 Chord 具有的基于 DHT 的资源搜索算法优势, 可利用环上每个节点唯一按序排列的身份标识 (identification, ID) 来实现快速资源定位, 并确保系统的

可扩展性和稳定性。DDNS在传统DNS服务器上以匹配给定域名和资源类型的资源记录集(resource record sets, RRSet)为查找对象,其记录的存储和检索通过DHT来实现。DDNS沿袭了DHash的特征,通过使用一致性哈希算法将每个阶段需要的密钥平均分配给所有节点,当其中某个节点在Chord环中进行资源记录的查询时,查询结果将进行缓存,因此当从 m 个节点组成的Chord环中找到某个特定记录时,每个节点传输给定记录的次数为 $\lg m$ 。同时,DDNS使用了签名机制,当新建或更新后的RRSet写入DHash时需要使用拥有者的私钥进行签名,当客户端检索RRSet时会利用对应的公钥验证该签名的有效性。另外,DNS条目以伪随机的方式复制,并沿着查找路径进行缓存,而且由于所有DDNS服务器都知道层次结构根的密钥(类似于DNS中所有服务器知道根服务器的IP地址),确保了每个客户端的请求都可以得到DDNS服务器的有效响应。虽然DDNS在继承了Chord的容错和负载均衡的特性基础上,克服了当前DNS存在的许多问题,但与传统的DNS相比,DDNS在延时和可扩展性等方面仍然不具有优势。

(2)P-DONAS^[59]

P-DONAS(a peer-to-peer (P2P)-based DNS)方案是对传统DNS的补充或替代,其核心思想是将为互联网提供DNS域名服务的站点作为访问节点(access node, AN),再基于Kademlia^[60]分布式哈希表技术,将AN组织成一个去中心化、自组织的P2P网络。每个AN扮演传统DNS服务器的角色,负责存储部分资源记录数据,同时直接为DNS客户端提供解析服务。P-DONAS作为一个中间件嵌入到传统DNS系统客户端与服务器端之间的中间层,当AN接收客户端的DNS查询请求时,先将该请求写入等待队列以免发生丢包,随后在本地缓存中进行查询,如果找到则直接返回客户端应答报文,否则在P2P网络中进行查询。在P2P网络中尚未找到的情况下,P-DONAS向传统DNS服务器发起查询请求,并将查询结果在返回客户的过程中逐级进行缓存。由此可以看出,在P-DONAS方案中,当客户端向AN发出DNS查询请求时,迭代查询过程通过P2P网络进行,而且在AN节点中没有找到查询记录时将向传统DNS服务器进行查询。该机制保持了与传统DNS系统之间的完全兼容与实时通信。通过仿真和实测,P-DONAS的性能与传统DNS相当,具有较高的可扩展性。

(3)CoDoNS^[61]

作为一种新型域名服务方式,CoDoNS(cooperative domain name system)是一个由分布在全球的CoDoNS

服务器组成的P2P网络。每个CoDoNS服务器担负着与传统DNS(legacy DNS)服务器相同的功能,采用与传统DNS相同的协议和数据传输方式,从而在不需要对DNS客户端解析器进行修改的情况下,实现与传统DNS之间的兼容性或直接从传统DNS平滑过渡到CoDoNS。如图3所示,当客户端发起DNS查询时,首先由CoDoNS服务器进行解析和应答,当CoDoNS服务器无法找到查询记录时便通过家节点(home node)向传统DNS发起查询请求,查询结果通过家节点返回客户端并在途经的服务器上缓存。由于家节点的存在,CoDoNS中的记录信息能够与传统DNS保持一致,并通过缓存机制在节点间进行复制。CoDoNS将DNS解析和名称空间的管理功能从传统DNS中解耦出来,域名持有者只需要从名称空间管理者获得用于代表该域名的证书并将其提交给CoDoNS,就可以完成域名在CoDoNS中的注册,同时传统DNS名称空间的层次结构以及管理策略对CoDoNS没有任何限制。CoDoNS通过构建在结构化P2P覆盖网络之上的基于Beehive^[62]的主动缓存机制来降低结构化DHT的平均查询延迟和时间复杂度,并通过自动负载均衡来提升抗DDoS攻击能力以及更新信息的传播速度。通过在PlanetLab开放平台上的部署与评估,CoDoNS具有低延迟、应对瞬间拥塞(flash-crowds)以及劫持更新的快速传播等功能。

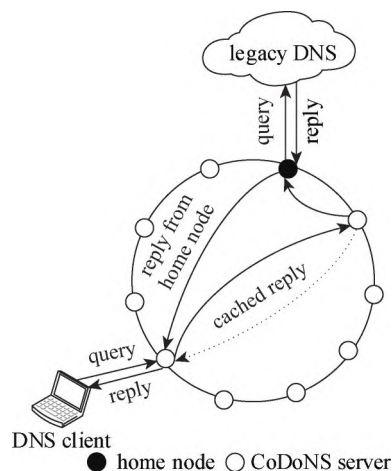


图3 CoDoNS结构

Fig.3 Architecture of CoDoNS

(4)HP2PDNS^[63]

HP2PDNS(hybrid peer-to-peer DNS)是使用基于P2P网络的DHT构建的一个开放的DNS。任何用户只需要在其中发布自己的分布式区域文件(distributed zone files, DZF),并用自己的私钥进行签名,就可以实现域名与持有者之间的身份绑定,并避免多个用户同时

关联一个域名现象的发生。HP2PDNS的设计目标是提供一个完全自由、自我管理和不受审查的DNS服务系统。如图4所示,HP2PDNS主要由包括转换器(translator)、代理(proxy)等组件的本地名称服务器(local nameserver)和P2P节点(P2P node)组成,另外还包括密钥管理(key manager)模块和黑名单(blacklist)管理模块。其中,客户端可以设置为本地名称服务器后通过转换器使用DHT进行域名解析,也可以通过代理使用传统DNS服务。同时,设置为本地名称服务器的客户端还可以定义DNS服务器的黑名单,并管理本地密钥。P2P节点模块与P2P网络进行通信,并从中检索用于保存域名资源记录及其公钥和签名的DZF。每个HP2PDNS客户端都是DHT中的一个对等节点,保存加入到网络中的其他节点的信息,同时充当客户端和服务端功能,向其他对等节点提供资源存储和通信功能。转换器用于将本地名称服务器接入P2P网络,由于本地名称服务器不知道如何读取DZF,这些工作都由转换器负责完成,而且转换器只接受用户已经安装了密钥的DZF,任何未经用户专门安装密钥的DZF都将被视为无效;当用户需要使用传统DNS服务时,则通过代理实现。DZF是HP2PDNS的核心,在没有中心化机制的约束下,用户很有可能会安装不正确的公钥或添加错误的DZF,进而成为网络钓鱼攻击的受害者。

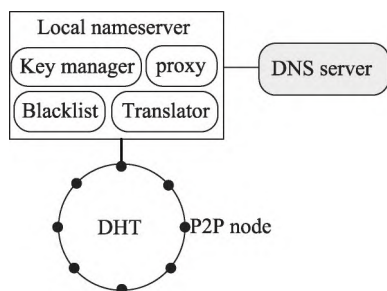


图4 HP2PDNS结构

Fig.4 Architecture of HP2PDNS

2.2 协议增强技术

DNS协议是指DNS客户端与递归解析服务器以及名字服务器之间实现查询与应答过程中所必须遵循的规则和约定。由于协议具有的规则、标准和约定属性,DNS协议增强技术的实现更加复杂且具有极大的挑战性。

(1) DNSSEC^[64-65]

设计DNS安全扩展(domain name system security extensions,DNSSEC)的初衷是应对因DNS架构在协议层最初并未提供安全措施而出现的缓存区中毒、DNS

劫持等攻击行为,主要是在DNS基础上借助基于公钥密钥机制的数字签名技术,通过对新引入的资源记录进行数字签名,从而为域名请求者提供真实和完整的应答信息。DNSSEC在传统域名系统中引入了DNS公钥(DNS signature,DNSKEY)、资源记录签名(resource record signature,RRSIG)、授权签名(delegation signer,DS)和NSEC3(next secure)4种新的资源记录。其中DNSKEY用于保存对区域签名进行验证的公钥,主要分为用于生成和验证域名的区域签名密钥(zone signing key,ZSK)和用于签名验证ZSK的密钥签名密钥(key signing key,KSK);RRSIG用于保存签名后的资源记录;DS存放资源记录的哈希值,用于验证DNSKEY的真实性,从而在不同区域之间建立信任链;NSEC3用于确定特定区域中是否存在某个名称,以应答不存在的资源记录。

DNSSEC的基本工作原理如图5所示^[66],以对www.test.net的域名访问为例,其工作过程主要包括:首先,递归解析服务器向权威名字服务器test.net发起访问www.test.net的查询请求;test.net向递归解析服务器返回一个应答报文,该报文除包含一个标准的www.test.net对应的IP地址的A记录外,还包含一个存放该域名数字签名的RRSIG记录;递归解析服务器为了完成对签名的验证,还需要从test.net处获得签名私钥对应的公钥;test.net将存放公钥的DNSKEY资源记录发送给递归解析服务器,然后递归解析服务器就可以验证www.test.net记录的真实性和完整性。为了防范攻击者伪造公钥(DNSKEY记录)和公钥的数字签名(RRSIG记录),DNSSEC采用了信任锚(trust anchors)机制,即由信任链中的父节点为其子节点的公钥哈希值进行数字签名,以

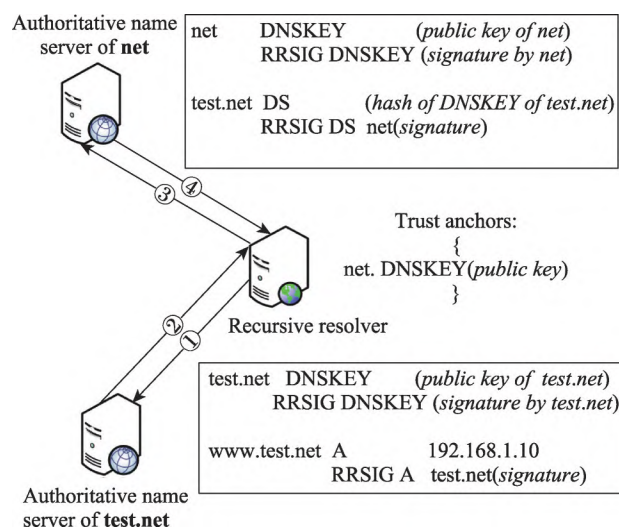


图5 DNSSEC基本工作原理

Fig.5 Basic working principle of DNSSEC

确保每个公钥是真实的。在本例中,递归解析服务器可以通过向 net 查询 test.net 的 DS 记录来验证其公钥的真实性。

DNSSEC 的核心是在传统 DNS 中通过数字签名来保证应答信息的真实性和完整性,与此同时也引入了针对中心化密钥分配和管理系统进行 DDoS 攻击的安全风险,而且额外添加的字段和加密信息也增加了系统实现的复杂性,因此 DNSSEC 在互联网中的实际部署(尤其在二级域名服务器以下的部署)并不理想。但由于 DNSSEC 技术在域名安全中的重要性,Internet 工程任务组(Internet engineering task force, IETF)在原有技术基础上进行了一系列改进和优化,并以 RFC(request for comments)文档形式发布,其中 RFC8080^[67]中采用了更加高效和安全的 Edwards 曲线数字签名算法(Edwards-curve digital signature algorithm, EdDSA),在 RFC8198^[68]中使用了 NSEC/NSEC3 资源记录以提高查询性能和隐私性,在 RFC9157^[69]中优化了 DNSSEC 算法和资源记录的管理方式。

(2) DNSCurve^[70-71]

由于 DNSSEC 并未取得预期的安全防护效果,研究人员提出了另一个力求消除已知 DNS 安全漏洞且能够提高 DNS 查询和响应机密性与完整性的实用系统 DNSCurve。具体讲, DNSCurve 通过在链路层加密所有的 DNS 查询和应答报文来实现机密性,并能够有效防范伪造 DNS 应答报文的攻击以及针对 DNS 服务器的 DDoS 攻击。

为了向后兼容传统 DNS, DNSCurve 在传统 DNS 报文基础上引入了新的协议规范,通过在 NS 资源记录(name service resource record)中嵌入服务器的公钥来实现与 DNS 相同的往返时间(round trip time, RTT)。其中, DNSCurve 使用了 Curve25519 椭圆曲线加密算法交换会话密钥,然后用于在缓存(递归解析服务器)与名字服务器之间提供身份验证和加密。如图 6 所示,当用 DNSCurve 解析 www.test.net 时,其工作过程为:①缓存通过向 net 服务器查询 www.test.net 对应的 NS 资源记录来协商用于加密通信的共享密钥;②当 DNSCurve 服务器接收到该查询请求后,使用 Base32 编码方式将自己的公钥嵌入到 NS 资源记录中,并返回给缓存;③缓存首先从 NS 资源记录中获得 DNSCurve 服务器的公钥,然后利用 DNSCurve 服务器的公钥、自己的私钥和一个一次性 nonce(用于防范重放攻击)创建一个共享密钥;④缓存将该共享密钥、自己的公钥和一次性 nonce 放到加密箱(cryptographic box),然后经 Base32 编码后以查询报文的形式发送给 test.net 服务器(部署了 DNSCurve);

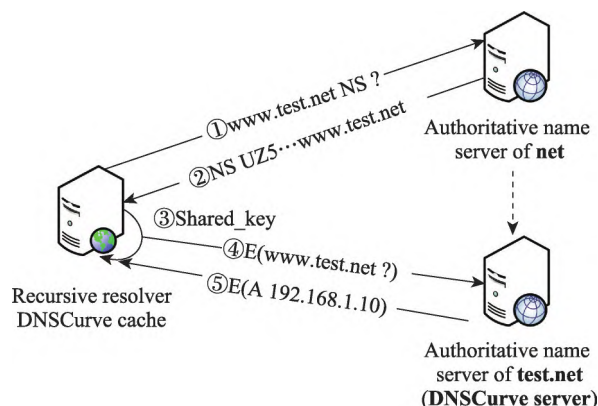


图6 DNSCurve 基本工作原理

Fig.6 Basic working principle of DNSCurve

⑤ DNSCurve 服务器从查询报文中得到加密箱,然后使用自己的私钥、缓存的公钥和一次性 nonce 生成 DNSCurve 服务器端的共享密钥,经验证正确后,将响应报文以加密箱形式经加密后发送给缓存,缓存最终将得到正确的响应。

虽然 DNSCurve 通过 Cryptographic Box、椭圆曲线加密(Curve25519)等关键技术为 DNS 查询和响应提供了高效、安全的加密和验证机制,且能够有效保护 DNS 通信的隐私性和完整性,并防范针对 DNS 服务的网络攻击,但其部署难度和系统开销较大,同时缺乏传统 DNS 和 DNSSEC 服务商的广泛支持,导致其发展缓慢。另外, DNSCurve 主要用于服务器之间的通信加密,而 DNSCrypt^[72]更倾向于 DNS 客户端与递归解析服务器之间的通信加密,两者在实现功能上可以相互补充。

2.3 实现过程增强技术

分布式系统、云架构、负载均衡、集群等技术都可以增强 DNS 系统的安全性,而本节重点关注于专门针对 DNS 协议在实现过程中的性能优化和攻击改进。

(1) CoDNS^[73]

CoDNS(collaborative DNS)是一种采用分布式技术实现的 DNS 解析系统,旨在通过服务器节点之间的相互协作来提高 DNS 解析的效率和可靠性。具体讲,在 DNS 客户端运行着 CoDNS 守护进程,客户端的 DNS 查询请求传递给 CoDNS 守护进程,CoDNS 首先尝试使用本地名字服务器进行解析,一旦解析超时将该查询请求转发给 P2P 网络中的其他名字服务器,并将超时阈值(原始超时阈值根据本地名字服务器的响应状态动态调整)加倍。当第 2 个超时阈值过期时,CoDNS 选择另一个对等服务器节点进行查询。CoDNS 重复此过程,获得解析结果后,名字服务器将结果返回给客户端,并更新本地及邻居节点缓存。CoDNS 只有当本地名字服

务器出现故障时才会向远端服务器发起查询请求。当前,在正常情况下 98%~99% 的查询都会在本地完成^[74]。因此 CoDNS 对系统的资源占用很小。

虽然 CoDNS 在可靠性和运行性能方面比传统 DNS 具有更大优势,但其安全性仍然很脆弱,任何错误的解析结果都会通过缓存机制传播到其他节点。为了解决此问题,ConfidDNS 系统^[75]重新设计了一套安全策略,用于检测并判断 IP 地址与域名映射之间的稳定性以及不同 DNS 解析器中同一域名查询结果的一致性。

(2) T-DNS^[76]

T-DNS (taobao DNS) 是阿里巴巴集团开发的采用分布式技术的一种高性能 DNS 系统,旨在提升传统 DNS 的安全性、可靠性和运行性能,主要应对大规模、高并发 DNS 查询请求。具体讲,T-DNS 通过引入 DoH (DNS over HTTPS)^[77]、DoT (DNS over TLS)^[78] 等加密技术来防止数据在传输过程中被窃取或篡改,从而有效抵御中间人攻击、DNS 欺骗等安全威胁;通过支持 DNSSEC 来确保查询结果的真实性和完整性;通过匿名化查询请求和限制日志记录方式来减少用户隐私信息的泄露,从而降低数据被滥用的风险;通过采用分布式架构和智能缓存机制,优化解析路径,减少延时,提高域名解析的效率;通过流量清洗、负载均衡等技术,提升防御 DDos 攻击的能力;通过支持基于地理位置、网络状况、用户策略的智能路由功能,优化对 DNS 服务器的选择并提升访问速度。尽管 T-DNS 在安全性、运行性能和隐私保护等方面都有明显改善,但 T-DNS 的实际部署过程中在复杂性、兼容性、系统开销、密钥管理、路由策略的公平性及其监管等方面仍然需要继续进行优化和改进,以实现更广泛的应用。

(3) DR-DNS^[79]

通常情况下,互联网环境中一般会配置主、备两台递归解析服务器分别为客户端提供 DNS 解析服务,容易遭受漏洞、虚拟查询和 DDos 攻击等安全威胁。分布式弹性 DNS (distributed and resilient DNS, DR-DNS) 摒弃了传统 DNS 的集中式分层结构,采用多节点分布式架构设计来提升传统 DNS 的抗攻击能力和可靠性。在 DR-DNS 中,DNS 管理程序同时在管理着多个 DNS 服务器软件副本,当客户端发起 DNS 查询请求时,DNS 管理程序将其分发给不同的 DNS 服务器软件副本。每个 DNS 服务器软件副本独立完成查询,并将结果返回给 DNS 管理程序,然后由 DNS 管理程序采用投票机制从返回结果中选出票数最多的一个返回给客户端,同时对该结果进行缓存。由于 DR-DNS 中的投票机制选择以票数的多少决定结果,在运行 $2t+1$ 个不同的 DNS 服

器软件副本时,能够保护客户端免受 t 个错误副本的攻击。虽然 DR-DNS 向后兼容传统 DNS 并便于系统的部署,但投票机制会在一定程度上影响查询的响应速度,另外系统复杂性增加,维护多个节点的一致性需要更多资源。

(4) OnionDNS^[80]

传统的 DNS 系统没有提供有效机制来防范非法域名查封 (domain seizures) 现象的发生,也没有对 DNS 查询和响应信息提供安全加密和隐私保护措施,DNS 查询结果容易遭受攻击而使其真实性和完整性无法得到保障。为解决此问题,OnionDNS 通过提供的一个匿名顶级域名 (TLD) 和互联网解析服务,采用强制缓存、隐蔽服务、DNSSEC 签名和 Tor 网络等技术来有效保护 TLD 安全性,为用户提供防范域名查封服务。

如图 7 所示,通过引入的镜像服务器和 .o 区域作为 OnionDNS 的顶级域名,来接管传统 DNS 系统中的 TLD,.o 区域接受根服务器的管理并同步数据,镜像服务器与 .o 区域之间通过 Tor 网络通信,从而隐藏 OnionDNS 根服务器的物理位置。当客户端通过开放的互联网或 Tor 网络向镜像服务器发起查询请求时,镜像服务器首先从本地缓存中寻找是否存在相应的记录,如果存在则直接返回域名对应的 IP 地址,否则返回域名不存在的响应报文。在此过程中,OnionDNS 镜像服务器在本地缓存中没有找到对应的记录时并没有采取传统 DNS 系统的迭代查询过程,而是根据本地缓存直接返回结果,同时镜像服务器通过 DNSSEC 协议周期性地从匿名 TLD 中获得 .o 区域的更新记录,从而保障记录的真实性,并对根服务器进行匿名保护。此外,客户端请求永远不会使镜像服务器向根服务器发起迭代查询,这将有效防止攻击者将流量注入 Tor 网络并使服务失去匿名化。由于 OnionDNS 部署和实现过程的复杂性,其性能受到了较大影响。

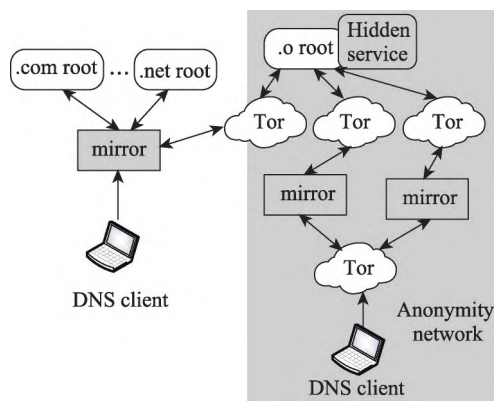


图7 OnionDNS 架构

Fig.7 Architecture of OnionDNS

(5)EncDNS^[81]

OnionDNS 为顶级域名服务器的安全提供了有效保护机制,但缺乏对客户端的隐私保护功能。EncDNS (encapsulated DNS) 的实现思路与 OnionDNS 有些类似,是一个以轻量级开源方式来提供低延迟并保护客户端隐私的 DNS 解析服务方法。其设计思想是在传统解析器 (conventional resolver, CR) 中运行一个代理程序,将客户端的查询报告加密后转发给 EncDNS 服务器。EncDNS 服务器对接收到的查询报告解密后,向传统 DNS 服务器发起迭代查询,然后将查询结果加密封装后返回给 CR 中的代理程序,最后代理程序将解密后的结果提交给客户端。

在 EncDNS 中,由 EncDNS 服务器接管传统 DNS 中由 CR 执行的任务,即 EncDNS 服务器执行实际的域名解析,在此过程中 EncDNS 服务器虽然能够学习到查询的域名,却无法学习到客户端的真实 IP 地址(因为查询来自于 CR 中的代理),从而实现了保护客户端用户隐私的目的。EncDNS 引入代理和加解密技术,将传统的单跳查询方式改变为两跳方式(第一跳为 CR 与代理,第二跳为代理与 EncDNS 服务器),虽然并没有改变传统客户端的工作模式,但需要通过修改 DNS 协议将经加密的消息封装在标准的 DNS 查询和应答报文中(CR 代理程序与 EncDNS 服务器之间采用 DNSCurve 协议),增加了系统实现的复杂性,不利于大范围部署。

2.4 小结

总体而言,传统 DNS 在设计之初没有充分考虑安全性,因此缺乏内生安全保护机制,同时随着应用功能的扩展,其伴生安全问题也逐渐显现出来。主要表现为:(1)因缺乏加密机制,数据在传输过程中被窃听或篡

改,存在域名劫持、缓存区中毒等中间人攻击威胁;(2)因使用 UDP 协议,而缺乏基于协议的验证机制,存在 DNS 查询的不可靠性,易遭受 DNS 欺骗攻击;(3)因缺乏足够的安全防护机制,针对 DNS 服务器(尤其是根服务器和顶级域名服务器)的 DDoS 攻击事件频发;(4)因域名注册系统存在的安全漏洞,攻击者可以通过社会工程学、凭证窃取或漏洞利用等方式篡改 NS 记录,存在域名注册信息被篡改的风险;(5)因 DNS 查询和缓存区记录通常采用明文方式,其信息易被第三方监控,存在隐私泄露风险。针对以上主要问题,研究人员提出了 DNS-SEC 等安全增强方案。表 3 分别针对主要增强方式、采用的核心技术、是否支持已有的 DNS 格式、客户端向后兼容性、抗 DDoS 攻击和缓存区中毒、隐私性、延时及应用实效等方面对主要方案进行了归纳总结。

3 区块链在 DNS 安全防护中的应用

区块链以其独有的去中心化、不可篡改、公开透明和可追溯等特性^[81],为有效应对传统 DNS 中面对的抗攻击性、数据完整性、身份认证等安全需求提供了技术支撑和基础保障。具体讲,利用区块链技术可以解决传统 DNS 因过度依赖层次化的服务器部署带来的单点故障与中心化风险;可以通过有效防范 DNS 解析数据篡改与缓存区中毒进而防御因中间人攻击而导致的域名劫持或流量重定向现象;能够通过有效弥补传统 DNS 中存在的身份认证缺陷而防范域名劫持和伪造域名注册信息等事件的发生,同时可以在较大程度上解决因 DNS 软件漏洞带来的安全威胁。本文根据在新方案中是否必须保留传统的 DNS,将区块链在 DNS 安全增强中的应用分为融入区块链的 DNS 安全增强方案和基于

表3 传统DNS安全增强方案分析与比较

Table 3 Analysis and comparison of traditional DNS security enhancement schemes

名称	主要增强方式	核心技术	支持已有 DNS 格式	向后兼容性	抗 DDoS 攻击	抗缓存区中毒	隐私保护	延时	应用实效
EDNS0	根服务器增强	报文动态探测	√	√	×	×	×	很大	广泛部署
DDNS	系统增强	Chord	√	×	√	√	×	大	原型系统
P-DONAS	系统增强	Kademlia	√	√	√	√	×	较小	原型系统
CoDoNS	系统增强	Beehive	√	√	√	√	√	较小	PlanetLab 系统部署
HP2PDNS	系统增强	DHT+DZF	√	√	×	×	√	较小	原型系统
DNSSEC	协议增强	数字签名	×	√	×	√	×	较大	大范围部署
DNSCurve	协议增强	链路加密	×	√	√	×	√	较大	小范围部署
CoDNS	实现增强	分布式计算	√	√	√	√	×	小	局部部署
T-DNS	实现增强	分布式计算	×	×	×	√	√	小	局部部署
DR-DNS	实现增强	分布式计算	√	√	×	×	×	较大	原型系统
OnionDNS	实现增强	Tor+DNSSEC	√	√	×	√	×	较大	局部部署
EncDNS	实现增强	代理+DNSCurve	×	√	×	√	√	较小	局部部署

区块链的 DNS 安全方案两类。前者是一种渐进性措施,利用区块链技术来优化传统 DNS 的功能以提升其安全性。后者则是一种颠覆性技术,利用区块链技术来重构域名系统,提供一套独立于传统 DNS 的全新的域名服务基础设施。

近年来,随着区块链技术的不断成熟以及应用领域的不断扩展,将区块链应用于 DNS 安全增强或重构安全的 DNS 系统成为研究的热点,本章通过对相关文献的搜索与梳理,针对不同的功能特点和应用场景,分别选取一些典型方案进行讨论。

3.1 融入区块链的 DNS 安全增强技术

根据区块链技术在 DNS 安全增强中发挥的作用,将融入区块链的 DNS 安全增强技术分为主要针对根服务器的安全增强技术和主要针对递归侧的安全增强技术 2 种类型。

3.1.1 主要针对根服务器的安全增强技术

传统 DNS 采用的分层结构和缓存机制在提高效率的同时,也引入了单点故障、中间人攻击、隐私泄露等风险,区块链技术可从不同层面解决或缓解当前 DNS 中存在的安全问题。由于根服务器在 DNS 系统中的极端重要性,将区块链应用于实现根服务器的安全增强显得非常重要和必要。

(1) RootChain^[82]

DNS 的分层结构决定着根服务器存在因单点故障带来的安全风险,而且根区文件的管理和结果发布缺乏透明性和可监管性。针对 DNS 根服务器运行和管理现状,Zhang 等人^[82]提出了一种基于区块链的分布式 DNS 根区管理架构 RootChain。RootChain 在设计上体现了 4 个功能特点:①保留传统 DNS 的单一根结构,实现与传统 DNS 之间的兼容;②根区操作由不同的操作人员跨

多个物理节点进行,避免单点故障;③实现对整个 TLD 的全生命周期管理,从而提供根区管理过程的透明性和可监管性;④对递归解析器透明,并在协议层实现了与 DNS/DNSSEC 的兼容。

RootChain 是一个由运行区块链节点的根服务器组成的许可链,通过将 TLD 的授权与 TLD 的数据发布剥离,在保留单一根权限的同时实现对 DNS 根区的分布式操作。根区操作的事务由根区管理机构和 TLD 管理机构提交给 RootChain,并记录在区块链分布式账本中。RootChain 中提供了 4 类主要的角色:①根授权(root authority)。在 RootChain 中只有一个根授权,同时扮演着当前 DNS 中的 ICANN 操作员、根区维护员和根区管理员的角色。除发布根区数据外,根授权机构还将 TLD 委托给指定的 TLD 授权机构,并根据根授权机构与 TLD 授权机构之间签署的合同约定来转让和撤销现有的 TLD 授权。②TLD 授权(TLD authority)。TLD 授权机构扮演着 TLD 注册机构的角色,根授权机构通过向 RootChain 提交 TLD 委托事务,将 TLD 委托给 TLD 授权机构管理。③根服务器操作员(root server operator)。根服务器操作员负责管理根服务器。RootChain 中的根服务器除作为授权域名服务器提供域名解析服务外,还根据区块链事务负责根区域管理。④用户(user)。RootChain 中的用户对应传统 DNS 中的递归解析器和存根解析器,向任意根服务器发送标准的 DNS 查询,获取 TLD 的 NS 和 A/AAAA 记录。

如图 8 所示,RootChain 中 TLD 的根区操作有 3 种类型,分别通过 3 种智能合约来实现:①委托操作(delegation operations)。根授权通过将 TLD 与 TLD 授权机构的公钥绑定,将 TLD 委托给具有发布操作权限的 TLD 授权机构。具体由 ICANN 向 TLD 授权机构发送

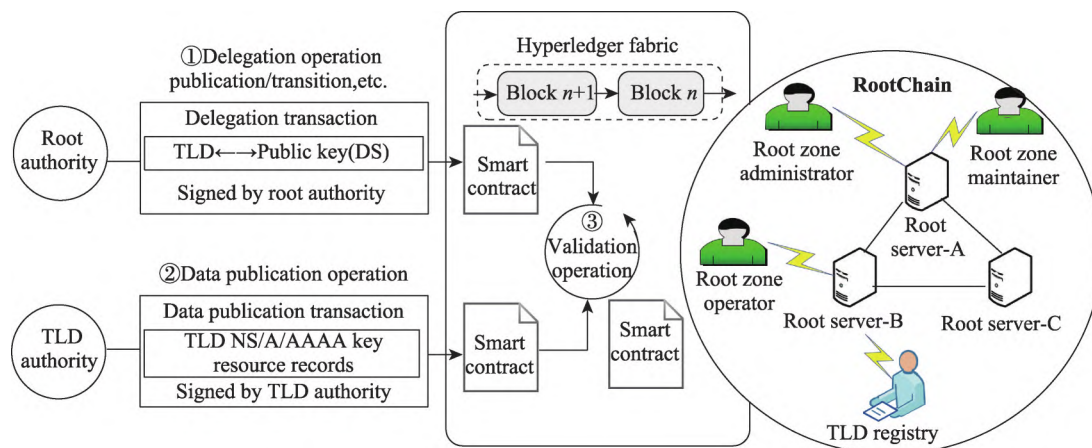


图8 RootChain 架构

Fig.8 Architecture of RootChain

委托授权请求,从而触发合约的执行,并将结果打包进区块后上链保存。②数据发布操作(data publication operations)。TLD授权机构通过向RootChain发送被签名的数据发布操作,用来发布被委托TLD的NS/A/AAAA资源记录。③验证操作(validation operations)。根服务器通过执行智能合约来验证委托操作(如发布、转变、撤销、续订、赎回等)和数据发布操作的有效性,智能合约强制根授权机构和所有TLD授权机构按照既定策略运行。为了实现以上3类操作,RootChain分别提供了3种对应的智能合约,所有操作结果保存在区块链上。

RootChain对递归解析器、存根解析器和DNS/DNSSEC兼容且透明,并在Hyperledger Fabric中开发了原型系统,且通过实验进行了评估。另外,为了摆脱传统分布式主节点(distribution master, DM)系统将根区数据从ICANN传输到根服务器时带来的安全问题,文献[83]设计了一种允许节点随时加入和退出的基于区块链的分布式DM结构,使用全新的共识算法来提高系统的安全性,利用灵活的签名机制来提高系统的性能。文献[84]提出了一种可依赖的基于许可链的分布式DNS根管理架构TD-Root。TD-Root中的每个根服务器通过共识算法维护一个在所有节点上都相同的根区文件,消除了目前集中式管理架构中的安全漏洞和信任风险。在此基础上,TD-Root中还使用了一种基于区块链数据结构的优化查询机制,以降低部署的复杂度和难度,同时在Go语言中实现了TD-Root。并通过Google云进行了仿真验证。

(2) Handshake^[85]

Handshake是一种基于未花费的交易输出(unspent transaction output, UTXO)交易模型的区块链协议,用于DNS系统中TLD的注册、续订和数据的安全传输。设计Handshake的目的不是取代传统的DNS系统,而是替代传统DNS系统中的根区文件和根服务器,使用区块链管理TLD的注册和解析,从而减少对中心化机构ICANN的依赖。通过区块链实现域名所有权的分布式管理,利用区块链的不可篡改性防止DNS劫持、域名欺骗等攻击,通过去中心化的分布式架构避免对域名的封锁或控制。

具体讲,在Handshake中区块链取代了传统DNS的根区文件,TLD(如.com、.org等)注册信息存储在区块链分布式账本中,用户可以直接在区块链上注册TLD而无需通过ICANN的审批。为了实现与传统DNS的兼容,现有主流的TLD(如.com、.org、.net等)的归属权仍然归传统管理机构(如VeriSign)。在进行域名解析时,客户端首先在手shake区块链上获取TLD信息,然后

通过传统DNS来解析子域名。Handshake可与传统DNS共存,未在区块链上注册的TLD请求会被转发到传统DNS根服务器。Handshake软件由全节点和轻量级客户端组成,全节点允许用户进行注册、更新、传输和域名解析,用户也可以使用全节点进行区块链支付,而轻量级客户端只允许用户解析域名。

Handshake采用改进的工作量证明(proof of work, PoW)共识算法,结合类似比特币的UTXO交易模型,以提高系统的安全性。在Handshake中,用户通过直接控制私钥来管理域名的所有权,不需要域名注册机构或证书颁发机构(certificate authority, CA)的参与,域名数据分布式存储在区块链中,以防止被删除或篡改。同时,Handshake兼容现有的DNS协议,用户可通过安装浏览器插件或直接使用Handshake的解析器(如NextDNS)访问Handshake域名。

目前,Handshake虽在兼容性和普及性上面临一定的挑战,但其技术路线和实现策略值得关注。

(3) D³NS^[86]

分布式去中心化域名系统(distributed decentralized domain name service, D³NS)是一个用于取代当前TLD服务和证书颁发机构的系统,提供更高的健壮性、安全性和可扩展性。针对传统DNS和DDNS中存在的突出问题,D³NS的功能优势主要体现在两个方面:一是在区块链上利用侧通道(side channel)方法来确认域名所有权,从而实现类似DNSSEC的安全功能;二是提出了一种经过优化的具有允许最小延时的DHT结构,使用DHT存储DNS记录。

为了提高消息的路由效率,D³NS提供了一个能够对网络路由进行实时优化的UrDHT^[87]。UrDHT基于P2P网络构建,节点平等参与数据存储与路由,通过将TLD的解析记录存储于UrDHT可以绕过ICANN的管控。D³NS将UrDHT提供的数据在经过区块链认证后再提供给指定的DNS服务器或客户端,实现与现有DNS协议的反向兼容。同时,位于D³NS系统中的DNS节点只会通过UrDHT交换数据,而不会从其他DNS服务器请求数据,确保DNS查询信息的可信性。UrDHT的成员也是区块链网络的节点,因此所有保存在UrDHT的记录在提交给用户之前都可以认为是合法的,从而避免了重放或注入攻击的发生。

D³NS利用类似比特币交易方式来记录域名所有权,当矿工在挖矿竞争中胜出后并没有获得代币奖励,而是得到了申请一个域名的权利。打包进区块的每一个交易表明矿工申请了一个新的域名或将某个已有域名的所有权转移到了自己名下。位于区块链上的每个

域名都可以与持有者的公钥进行绑定,由私钥验证域名持有者的合法性。用户向设置为DNS网关的计算机(该计算机是UrDHT和挖矿网络的成员)发起查询请求,如果该查询记录保存在UrDHT中,并且在区块链中已经建立了域名的持有者,则用存储的DNS记录进行应答,否则将回复DNS请求失败。

D³NS虽然在抗审查、隐私保护及资源动态管理场景中具有独特优势,但在大规模环境下运行时还需要在性能、兼容性、用户体验等方面进行优化,以实现技术的落地。

(4)IDV^[88]

针对DNSSEC在政治、经济、技术等方面存在的限制,Hu等人^[88]认为传统DNS系统的最大局限性是体系结构和管理模式的中心化。同时,受内容分发网络(content delivery network,CDN)^[89]加速原理的启发,提出了一种基于CDN的域名真实性验证方法——基于区块链的互联网域名验证(Internet domain name verification based on blockchain,IDV),该方法使用联盟链代替根域名服务器来验证域名的真实性,避免了单点故障和单边控制风险。

IDV的实质是一套验证系统,由部署在CDN缓存服务器上的验证服务和部署在用户终端上的域名验证客户端组成。其中,在DNS客户端上部署一个域名验证守护进程,作为DNS客户端主机的后台进程运行,负责监控本地DNS缓存。当验证守护进程发现本地DNS缓存中出现新的域名解析结果时,立即向验证服务器发送该域名验证请求。当验证服务器接收到域名验证请求时,将在本地完成域名的真实性验证,并将验证结果返回给客户端。通常情况下,当客户端访问一个新域名时,需要通过传统DNS系统进行域名解析。一旦客户端完成新域名解析,解析结果将会被缓存到CDN缓存服务器中,并在后续域名解析过程中提供真实性验证服务。在IDV中,区块链技术发挥的主要作用是将多个CDN缓存服务器组织成一个联盟链,不同CDN缓存服务器之间通过P2P网络实现相互间的通信,CDN服务器通过智能合约完成对域名的验证,防止恶意CDN服务器提供虚假的验证结果。

与DNSSEC相比,IDV对域名验证流程进行了简化,将DNS数据平面的功能迁移到了区块链,提高了域名解析和验证的效率,而且不存在单点故障和单边控制风险。同时IDV可以增量部署,互联网服务提供商可以利用位于网络边缘的CDN服务器来为客户端提供域名缓存服务,并通过轻量级算法完成域名真实性验证操作。另外,由于CDN业务已经在全球范围内得到了广

泛部署,而且CDN服务可以将DNS解析流量重定向到靠近的缓存服务器,从而减少网络访问延时。为此,IDV部署的可行性要比DNSSEC高,但IDV中作为区块链节点的CDN缓存服务器负责对客户端发出的DNS解析请求进行实时监控,一旦找到新的域名解析结果便进行本地缓存。在此过程中,CDN缓存服务器如何对一个新的域名请求结果的真实性进行验证,还需要借助区块链之外的验证机制来完成,不但增大了响应延时,而且引入了新的安全风险。

3.1.2 主要针对递归解析服务器的安全增强技术

由于递归解析服务器在DNS系统中所处的特殊位置及其具有的功能属性,成为各类网络攻击的主要目标及安全问题频发的关键位置,如缓存区中毒、DDoS放大攻击、隐私泄露、软件实现漏洞等。利用区块链分布式账本提供的数据存储、密钥管理、签名验证等技术可以有效解决递归服务器侧存在的安全问题。

(1)B-DNSSEC^[90]

基于区块链的DNSSEC(blockchain based DNSSEC,B-DNSSEC)是一种采用区块链技术的旨在提供与DNSSEC相同安全性能的域名系统。由于DNSSEC需要一条到根服务器的信任链,请求数量过多,从而影响签名的效率。如果域名直接以可信的方式绑定到公钥,就可以从系统中去掉这条信任链,区块链技术正好提供了这一功能。虽然公开密钥基础设施(public key infrastructure,PKI)^[91]是目前互联网上公认的信息安全基础设施,但其密钥分发与管理过程中存在的效率和安全问题一直被诟病。X509Cloud^[92]架构允许将PKI中的X.509证书添加到公共区块链网络,证书不仅可以像PKI那样直接发送给申请者,也可以在X509Cloud网络广播。系统中的每个CA都可以验证证书的有效性,一旦代表资源记录的交易被验证,将被打包进区块并上链保存,为资源查询提供验证服务。

在域名查询的每个阶段,X509Cloud区块链网络都充当着安全和可信的存储器角色,根KSK不再作为信任锚,那里缓存了名字服务器的A记录,解析就从那里开始。图9所示的是查询www.test.net对应的IPv4地址的过程,其中:

①与传统DNS查询一样,客户端启动对www.test.net的正常查询,该查询请求被转发到递归解析器。

②~④递归解析器向各名字服务器迭代查询得到www.test.net的一个A记录及签名。

⑤递归解析器在X509Cloud区块链网络中搜索www.test.net证书的最新条目,检查证书的有效性,并对签名进行验证。

⑥经过验证的A资源记录将被转发给客户端。

通过融入区块链技术,B-DNSSEC利用存储在区块链上的证书链对域名身份进行签名验证,从协议层面实现了对DNSSEC的功能优化和安全增强。B-DNSSEC对DNSSEC完全兼容,可作为DNSSEC的一个功能扩展集进行部署。由于B-DNSSEC中的签名算法是开放的,可以选用目前区块链网络中安全性较高的椭圆曲线数字签名算法(elliptic curve digital signature algorithm, ECDSA)来替代早期的RSA算法,但如何平衡效率与安全是未来一个重要的研究方向。

(2) TI-DNS^[93]

TI-DNS(trusted and incentive DNS)是一个基于区块链的可信激励DNS解析架构,主要用于防御DNS缓存区中毒攻击。具体讲,TI-DNS的主要特点体现为:

①可信(trusted)。每个TI-DNS网络维护一个全局唯一的区块链分布式账本,作为解析器的验证缓存(verification cache)。为了实现可信性,TI-DNS设计了一个由智能

合约实现的多解析器查询投票机制,以验证每个记录的创建或更新操作,且实现了操作的透明性和可追溯性。②激励(incentive)。设计了一种称为选民选择(voter selection)的共识算法,对历史行为较好的参与者给予更大权益,并激励其参与决策。③高效(efficient)。通过查询区块链中的记录来验证授权响应,不需要加、解密过程。④真实(practical)。只需要修改现有DNS系统的解析器,不需要设计新的交互协议或引入新的资源记录类型,可兼容DNSSEC。

TI-DNS主要由递归解析器和区块链平台组成,其中作为DNS解析入口的递归解析器同时还扮演着验证缓存和区块链节点的角色,而区块链平台中的分布式账本作为验证缓存为解析器提供验证服务。TI-DNS的关键技术是对解析器得到的DNS响应进行验证,并将经过验证的DNS记录保存在验证缓存中,而验证缓存是一个基于区块链的分布式账本,由所有参与者(解析器)共享和维护,如图10所示。TI-DNS的主要工作步骤为:

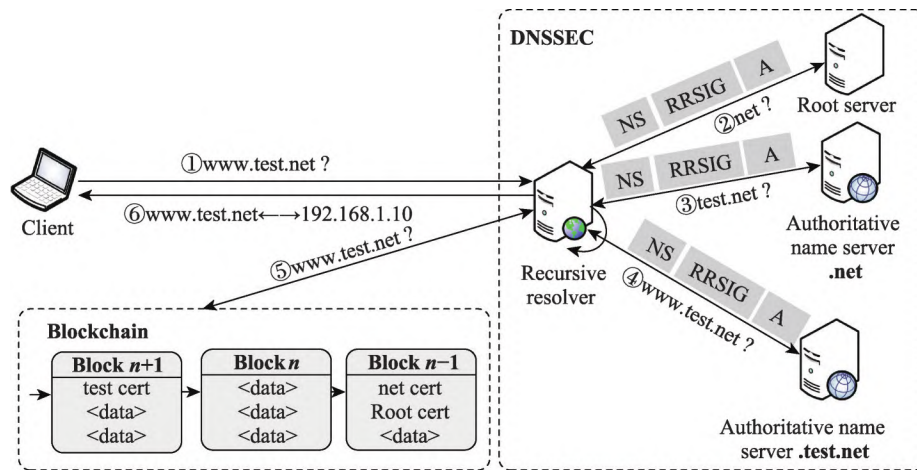


图9 B-DNSSEC协议执行过程

Fig.9 Implementation process of B-DNSSEC protocol

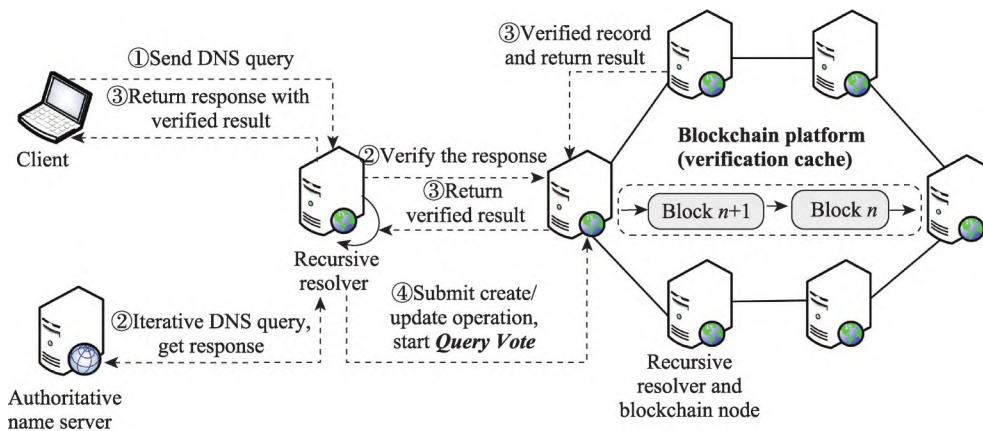


图10 TI-DNS系统架构

Fig.10 System architecture of TI-DNS

①客户端向递归解析器发送 DNS 查询请求。

②递归解析器从权威名字服务器接收到查询响应后,向位于区块链平台中的验证缓存进行验证。

③验证缓存完成验证操作,并将验证结果发送给递归解析器,递归解析器再返回给客户端。其中,如果结果为未通过(unverified)时,先前验证的记录将同时发送给递归解析器和客户端。

④递归解析器通过调用智能合约的创建或更新操作来提交新记录,并通过启动后续的查询投票(query vote)过程来验证其真实性。

TI-DNS 主要是利用区块链技术来检测和纠正因缓存区中毒攻击而引发的伪造 DNS 记录现象,主要包括多解析器查询投票方法和利益相关的激励机制,保证区块链账本上验证记录的可信性。TI-DNS 的功能实现只需要修改当前 DNS 解析器端,对系统的开销较小。另外,文献[94]提出的基于联盟链的 DNS 缓存资源可信共享模型(DNS cache resources trusted sharing model, DNSTSM),通过建立一条可信赖的区块链来存储域名记录并对解析过程进行验证,保证了域名解析结果的可信性。DNSTSM 的实现思路与 TI-DNS 类似,但两者都因区块链自身的性能以及频繁的验证过程带来的响应延时限制了其大规模推广应用。

(3) DNS-BC^[95]

DNS 系统通常由递归解析器、根名称服务器、TLD 名称服务器和权威名字服务器 4 类服务器组成。其中,后 3 种服务器存储实际记录,而递归解析器通常维护一个缓存系统来负责查询其他 3 种类型的服务器并响应客户端的请求。在 4 种类型的服务中,递归解析服务是 DNS 系统安全的关键,由于递归解析器的工作过程基于缓存机制,而 DNS 缓存系统存在实时性低和准确性差等缺陷,同时存在一些致命的安全和隐私问题。为了提高 DNS 缓存系统的性能并解决安全和隐私问题,Gao 等人^[95]提出了一种基于联盟链的缓存系统,即 DNS-BC。

DNS-BC 的典型结构如图 11 所示,递归解析器在接收到客户端的 DNS 查询请求后,首先检查其缓存。如果缓存中有请求的记录,递归解析器直接向客户端给予响应,否则,将执行迭代查询过程。迭代查询结束后,解析器将得到完整的 DNS 记录,在将其返回给客户端的同时,根据需要更新本地缓存。其中,为了加强数据传输的安全性,专门设计了 DoK(DNS over KCP^[96])协议,同时缓存的记录存储在联盟链上。该联盟链的节点由所有经过身份验证的名字服务器和递归解析服务器维护。联盟链中的每个成员都拥有描述节点可信度的评

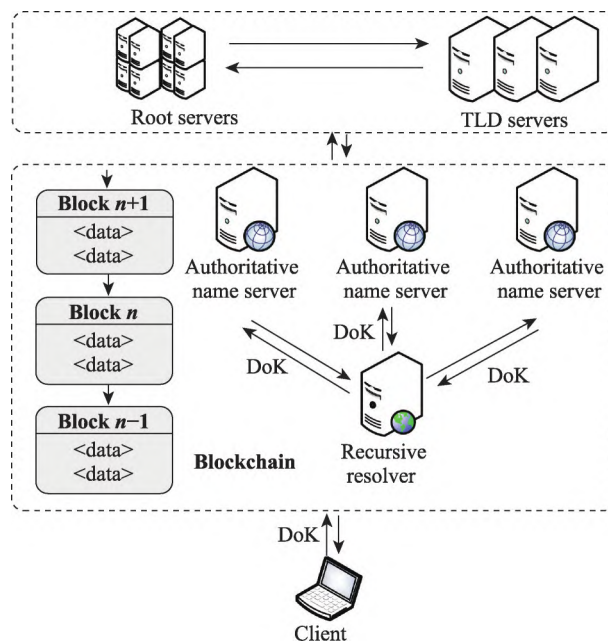


图 11 DNS-BC 的结构

Fig.11 Architecture of DNS-BC

分,客户端会优先选取可信度评分高的节点提供的缓存服务。系统规定,权威名字服务器的可信度评分为 1,而递归解析服务器的可信度评分均小于 1。另外,DNS-BC 系统提供了 3 大模块来实现其特有功能,其中数据存储模块(data storage module)用于存储 DNS 记录、各联盟链组成节点的可信度评分和各节点信息;数据处理模块(data handling module)负责记录查询、缓存更新和缓存的正确性验证等操作;服务模块(service module)负责维护每个节点的可信度、节点身份认证和颁发证书。

在 DNS-BC 系统中,由于客户端以及组成联盟链的递归解析服务器与权威名字服务器之间的通信都基于 DoK 协议进行,避免了 DNS 泛洪、DNS 放大、DNS 缓存区中毒、DNS 劫持等攻击的发生,提高了节点之间通信的安全性。但 DoK 协议在工作过程中需要利用彼此的公钥来验证双方的身份,并对数据进行加密处理,增加了协议实现的复杂性及通信延时。如何优化共识算法,并选择最适合的非对称加密算法应用到 DoK 协议,同时如何在安全性和延时容忍性之间取得最佳平衡,仍然是下一步的研究重点。

与 DNS-BC 不同,Chen 等人^[97]提出的 DagGridLedger 系统主要在递归解析服务器端引入了区块链技术,并基于大数据架构设计了一种新的冗余 DNS 协商和共识机制,实现了与传统 DNS 系统的兼容。具体讲,DagGridLedger 是一个基于分片机制的有向无环图(directed acyclic graph, DAG)^[98]区块链,它将区块链分片技术与 DNS 解析器端的 DAG 技术相结合,从而实现

DNS 解析过程的安全性和稳定性。DagGridLedger 中的每个节点共同维护一个链结构,用于保存查询记录,节点之间采用委员会共识算法将查询记录打包进区块后形成用于后续查询的缓存记录。

3.2 基于区块链的 DNS 安全方案

融入区块链的 DNS 安全增强方案的实现思路是利用区块链技术独有的功能去改造传统的 DNS 系统。虽然该方法有效提升了 DNS 系统的安全性和隐私保护能力,但仍然没有完全摆脱传统 DNS 系统架构和协议实现过程中带来的安全和隐私问题。体系结构固有的问题只能通过系统重构来实现,基于区块链的 DNS 安全方案完全放弃了传统 DNS 架构,将其功能置于由区块链主导的全新环境中来实现。

(1) Namecoin^[99]

Namecoin 是一个基于比特币(Bitcoin)技术的通过键/值(key/value)对实现域名注册和转移的域名系统,也是全球第一个开源的基于区块链技术的域名系统。从区块链技术的角度看,Namecoin 是一种通过比特币的分叉实现去中心化命名空间的加密货币,是比特币中第一个拥有自己区块链的山寨币。它提供了与比特币相同的功能,增加了一个可用于保存各种类型数据的名称/值(name/value)对存储方式,即用 Namecoin 中的名称/值对来替代比特币中的交易数据。Namecoin 使用了相当于 DNS 分层结构中的一个名为 .bit 的 TLD 作为命名空间,具体在名称子空间 ID 的前面加上“d”,即“d/example”。对于传统 DNS 来讲,Namecoin 使用了虚拟的 .bit TLD,但 .bit 并未真正被 ICANN 注册到 DNS 系统中。

与比特币不同的是,Namecoin 是一个可以用来注册名称/值对的命名空间。其中,注册过程利用 Namecoin 提供的 3 个脚本 NAME_NEW、NAME_FIRSTUPDATE 和 NAME_UPDATE 来完成,这些名称/值对存储在区块链后可以在个人之间进行交易。用户通过 Namecoin 客户端发起交易,将域名(如 d/example)写入区块链并给矿工交付一定的交易费(Namecoin 代币)。用户运行 Namecoin 客户端程序,直接查询区块链中的域名记录,解析过程由区块链直接提供,不需要依赖于中心化机制,而且域名数据不可篡改,除非私钥泄露或域名所有者主动更新。当需要对域名进行更新时,更新操作通过发送新交易完成。.bit 利用区块链技术确保网络中的每一个客户端都拥有相同的名称信息,而且任何人都无法非正常地修改任何信息,同时 .bit 不能轻易被审查。Namecoin 与传统 DNS 完全不兼容,但 DNS 客户端可以使用 NCDNS^[100]等桥接器来使

用 Namecoin。

Namecoin 与比特币有许多相似之处,包括相同的 PoW 共识算法、代币发行上限、区块创建时间以及交易操作等。Namecoin 支持与比特币合并挖矿(merge mining),这为 Namecoin 防范 51% 攻击提供了保障。Namecoin 通过相应的收费机制和协议来激励用户参与其中,用户在申请域名时需要向矿工支付一定数量的交易费。

在目前传统 DNS 安全问题尚未引起普遍不满的情况下,Namecoin 这一替代方案并未产生预期的应用效果,但其为有效防止潜在的中央权威滥用提供了有价值的参考,而且可以在一定程度上防止别有用心的人利用 .bit 为 Tor 或隐形网计划(invisible Internet project, I2P)^[101]匿名网络中的站点提供服务。就 Namecoin 应用中遇到的问题来看,域名抢注是一大难题,在检测的 12 万个注册域名中,只有 28 个没有抢注^[102]。另外,受一方控制的矿池所集中的算力很容易对当前的 Namecoin 形成 51% 攻击威胁。需要说明的是,Namecoin 还支持其他类型的数据存储,只是 .bit 是其中较为有影响力的应用。

(2) Blockstack^[103]

受 Namecoin 的启发,Ali 等人^[103]设计和实现了一个新的基于比特币的命名和存储系统 Blockstack,旨在取代传统 DNS 的根区域,并为用户提供了注册任意字符串作为替代性顶级域名(alternative top-level domains, alt-TLD)的能力。Blockstack 允许用户出售自己已经注册的 TLD,而不是 TLD 下的二级域名。与 Namecoin 不同的是,Blockstack 实现了控制平面与数据平面的分离。其中,控制平面定义了用于注册名称、创建名称与哈希值之间的绑定以及创建与管理密码对的协议,数据平面负责数据的存储,并为数据的可用性提供服务保障。区块链中只保存有代表数据哈希值和状态转换的元数据,而实际产生的数据以链下方式存储。

图 12 所示的是 Blockstack 的体系结构,由区块链、虚拟链、路由和存储 4 层组成。其中,区块链层提供了将操作顺序打包进区块的共识算法,同时操作被编码在交易中;虚拟链层在不需要更改底层区块链的基础上定义了新的操作以及接受或拒绝区块链操作的规则,这些操作作为额外的元数据编码在交易中,接受的操作由虚拟链处理,以构建一个用于存储全局状态信息以及任何给定区块状态变化的数据库。同时,虚拟链层引入了一个状态机来表示命名系统的全局状态,来自底层区块链的交易处理作为状态机的输入,有效地输入触发状态更改;路由层使用与传统 DNS 相同的区域文件形式存储路由信息,虚拟链将名称绑定到各自的哈希值(区域文

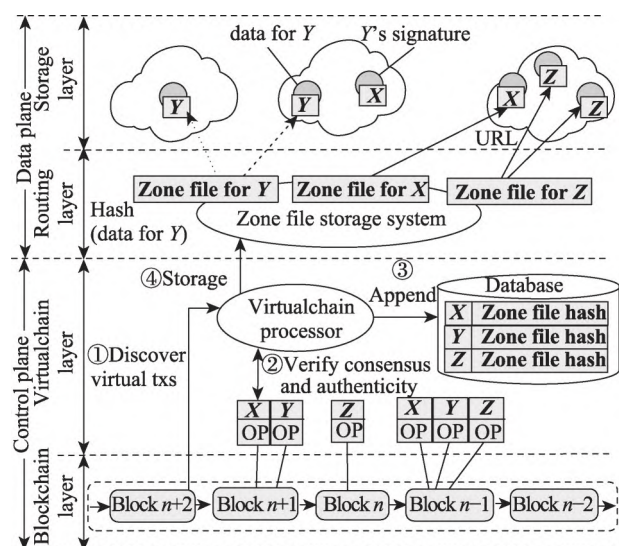


图 12 Blockstack 的 4 层结构

Fig. 12 4-layer architecture of Blockstack

件)后存储在控制平面中,而区域文件本身存储在路由层;最上端的存储层以名称/值对的方式存储实际数据,所有存储的数据值都由对应名称所有者的私钥进行了签名。由于数据值以链外方式存储在不同的后端,这样数据值的大小和具体存储位置将不受限制,而且用户只需要在控制平面验证数据值的完整性,而不需要信任存储层。

Blockstack 的设计不仅大大增加了系统的数据存储容量,而且允许每一层独立于其他层拓展和改进。Blockstack 声称自己是唯一拥有轻量级 DNS 递归解析器的命名区块链,用户可以通过插件方式将其嵌入浏览器、应用程序或设备^[104],但这种轻量级解析器为恶意软件提供了所需要的寄生环境,攻击者可以利用 Blockstack 中的分布式存储空间来存储攻击代码。

(3) ENS^[105]

以太坊名称服务(Ethereum name service, ENS)是基于以太坊的一个分布式、开放和可扩展的命名系统,提供了从人们可理解的名称(如 Alice、Bob 等)到机器可直接识别的标识符(如以太坊地址、内容哈希值、加密货币地址、元数据等)之间的转换。同时,ENS 还支持反向解析(reverse resolution)功能,实现主名称(primary name)、接口描述等元数据与以太坊地址之间的关联。ENS 可以实现与现有 DNS 之间的无缝对接,同时 ENS 支持通过 DNSSEC 导入 DNS 域名,允许将 .com、.xyz 或 .art 等域名导入 ENS 生态系统。由于 ENS 采用分层结构,拥有任一级别域名的用户都可以根据需要在其下创建子域,如 Alice 在其拥有的域名 .alice.eth 下创建子域 sub.alice.eth。

ENS 的实现依赖于注册表(registry)、解析器(resolver)和注册器(registrar)3 类智能合约,其中注册表以键/值对的方式记录所有域名及其关联信息,解析器通过标准化接口负责将域名映射到实际标识符,注册器通过竞拍或租用模式来管理域名的注册和续费规则。顶级域名(如 .eth、.test 等)由注册器智能合约拥有。每个 ENS 的域名可以是一个非同质化代币(non-fungible token, NFT)^[106],域名所有权可以通过转移 NFT 来实现。如图 13 所示,ENS 类似于当前的 DNS,客户端输入 alice.eth 域名,钱包将其转换为解析指令;ENS 注册表获取并向客户端返回域名的解析器地址;客户端向解析器请求目标记录(如以太坊地址),解析器返回结果。

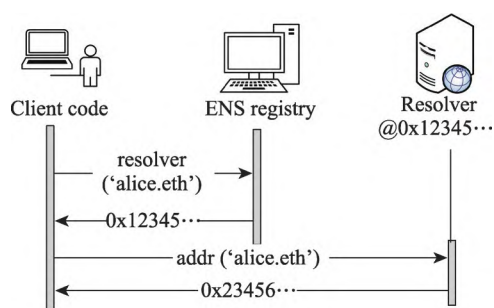


Fig. 13 ENS domain name resolution process

ENS 的域名数据存储在以太坊上,无法被篡改,同时注册信息公开透明,用户可以通过代理地址保护隐私,而且 ENS 通过多链解析器支持不同区块链地址。但是,ENS 客户端仍然需要进行域名解析,通过不安全的 UDP 协议与解析器对话,这其间存在中间人攻击的安全风险。同时,ENS 在域名解析过程中需要调用多次智能合约,而合约漏洞可能会导致域名被篡改。还有,ENS 的离线解析需要频繁地在以太坊节点与轻节点、第三方服务节点之间进行信息交换,将会影响域名解析的速度和可用性。

ENSv2^[107]是 ENS 的升级版本,旨在通过技术架构优化和扩展功能,提升域名服务的效率和用户体验。主要表现为:ENSv2 将域名注册与管理等功能从以太坊主网(Layer1)迁移到了 Layer2,通过支持跨链操作使域名解析与其他类型的区块链无缝对接,提供更加灵活的子域名管理工具,强化了与去中心化身份(decentralized ID, DID)^[108]的整合,增强的反向解析功能支持更多类型的链上数据(如 NFT 资产、社交账号等)的绑定,提升了域名实用性。

(4) EmerDNS^[109]

EMC(EmerCoin)^[110]是一个提供多种去中心化服务

(如域名系统、SSL/TLS 证书服务、存储解决方案等)的区块链平台,用户能够通过提供的去中心化软件开发工具包(decentralized software development kit, dSDK)在平台上进行项目的快速开发。EmerDNS 是 EmerCoin 区块链平台提供的一个去中心化域名系统,用于替代传统 DNS 系统。其中, EmerDNS 的运行完全依赖于 EmerCoin 区块链,域名注册与管理以及解析记录的更新等操作通过 EmerCoin 的智能合约实现,确保规则透明且不可篡改。EmerDNS 的结构如图 14 所示,主要由客户端、EmerDNS 服务器和 EmerCoin 区块链 3 部分组成,相互之间形成一个操作过程的闭环。

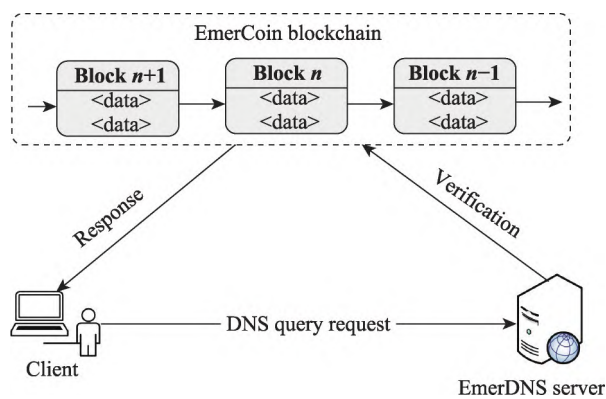


图 14 EmerDNS 结构示意图

Fig.14 Architecture of EmerDNS

EmerDNS 提供了去中心化、抗审查的域名解析服务,除记录所有者外,域名记录不能被任何人更改、撤销或暂停,只有记录所有者(拥有域名的私钥)才能修改或将其转移给另一个所有者。这些操作通过 EmerCoin 钱包中的名称/值存储(name/value storage, NVS)执行,也可以利用 EmerCoin API 来完成操作。DNS 记录可以通过 EmerCoin API 或 EmerCoin 钱包内置的标准 DNS 协议来检索。从技术上讲, EmerDNS 支持任何 DNS 区域或 TLD,但是为了实现与现有 DNS 之间的兼容,建议仅在区域中创建 .emc、.coin、.lib、.bazar 等记录。EmerDNS 内置了 A、AAAA、NS 等传统 DNS 的记录,并将这些记录写入到 EmerCoin 区块链,客户端可以通过浏览器功能扩展(安装插件)或使用 OpenNIC^[111]等工具来访问 EmerDNS 域名。另外,可以将 EmerDNS 服务器集成到传统 DNS 分层结构中,这样,既可以独立使用 EmerDNS 提供的服务,也可以使用传统 DNS 的缓存机制,只是现有的 DNS 客户端必须配置额外的 DNS 代理服务器。

EmerDNS 的特有应用场景主要有:可以将注册域名指向 Tor 或星际文件系统(interplanetary file system, IPFS)^[112]托管的网站,避免传统 DNS 的封锁;企业使用

EmerDNS 实现内部域名的管理,并结合 SSL 协议实现加密通信,防止中间人攻击。但 EmerDNS 目前遇到的挑战是用户普及率低(注册用户数远低于 ENS)以及浏览器兼容性差(需要安装插件)。同时, EmerDNS 和 Namecoin 都是基于比特币构建的命名系统, EmerDNS 与 Namecoin 一样遭受着域名抢注和被滥用的威胁。2021 年, Casino 等人^[113]收集了 EmerDNS 和 Namecoin 中的所有记录,在经专门的威胁情报机构分析后发现超过 50% 的 IP 地址被至少一个机构标记为恶意 IP。

(5) B-DNS^[114]

基于区块链的 DNS (blockchain-based DNS, B-DNS)通过构建权益证明(proof of stake, PoS)共识算法和域索引(index of domains)来解决当前融入或基于区块链的 DNS 存在的计算量大和查询效率低的问题。B-DNS 将 DNS 记录以交易方式存储在区块链中,并利用索引加速记录的查询。同时, B-DNS 与传统 DNS 系统兼容,即递归解析器和用户可以直接与 B-DNS 名称服务器交互。

图 15 所示的是 B-DNS 的 4 层架构,采用分层结构的好处是层与层之间形成松耦合关系,具有良好的可扩展性。其中,数据层(data layer)负责将 DNS 记录以交易方式打包进区块并上链存储,同时为了应对 DNS 记录注册、更新和撤销操作的需要, B-DNS 提供了一种称为操作记录(operation records)的新格式来存储资源记

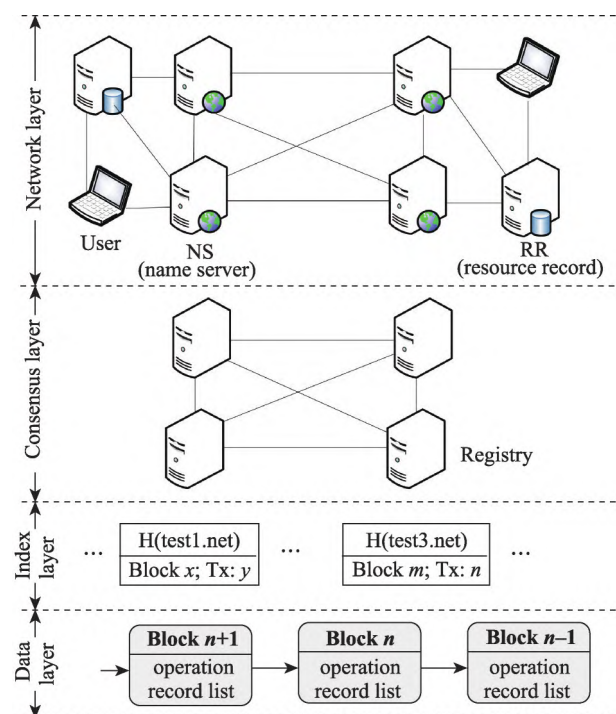


图 15 B-DNS 的 4 层结构

Fig.15 4-layer architecture of B-DNS

录(resource record,RR)。索引层(index layer)维护一个索引,以提高查询速度。B-DNS通过构建一个索引树,以键/值(key/value)对方式将域名映射到对应的IP地址,其中键是域名的哈希值,值是对应的IP地址。共识层(consensus layer)采用了PoS共识算法,保证DNS记录的一致性。在每个窗口期(epoch)执行一个领导(leader)选举函数,选择生成区块的节点(矿工)。同时,通过提出的一个有偏向抛币协议(biased-coin flipping protocol)和一个分布式随机数生成(random-number generation, DRG)协议来构建低算力要求的PoS共识算法。网络层(network layer)提供P2P连接,不仅可以与对等节点通信,而且可以向解析器和终端用户提供域名服务。

另外,PeerName^[115]为所有基于区块链的新域名注册提供了一个平台,DNSonChain^[116]是一种兼容传统DNS的基于区块链的名称服务系统。

(6)FI-DNS^[117]

由于在授权服务器副本之间以及父与子服务器之间缺乏强制数据同步机制,DNS系统存在不同节点之间的数据不一致、不同步等问题。针对此问题,Liu等人^[117]提出了一种新的基于区块链的域名解析和管理架构FI-DNS。FI-DNS在提供了域名解析过程中记录的可用性和一致性的同时,还利用公钥加密技术保证了域名结果的真实性和完整性,并通过支持基于智能合约的根区协同管理机制,实现了与传统ICANN分层结构的兼容。

域名解析的可用性问题是域名的授权服务器无法响应域名解析请求,而域名解析的一致性问题是域名的资源记录集(resource record set,RRSet)在不同的存储位置不一致。域名解析的不一致问题主要表现为3种状况:一是父区域中的胶水记录(glue records)与子区域中不一致,此现象称为跛脚授权(lame delegation)或授权不一致(delegation inconsistency);二是同一RRSet在不同授权服务器副本之间不一致,此现象称之为副本不一致(replica inconsistency);三是递归解析器中缓存的RRSet与权威服务器中存储的RRSet不一致,此现象称之为缓存不一致(cache inconsistency)。上述3类不一致问题产生的根源是DNS系统将域名的RRSet存储在多个副本权威服务器或缓存服务器中,同时传统DNS体系结构中缺乏一种内在机制来确保不同存储位置上RRSet的一致性。

图16显示了传统DNS分层结构与FI-DNS架构之间的对照关系。其中FI-DNS由两层分布式网络组成,第一层为有权限的区块链网络,而第二层为无权限的分

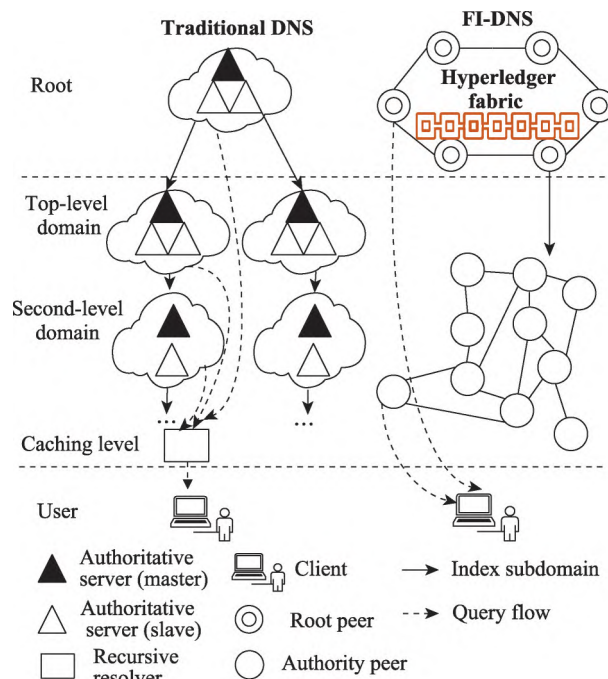


Fig.16 Structure comparison between traditional DNS and FI-DNS

布式文件系统。第一层是由根对等节点组成的联盟链,根对等节点扮演着传统DNS中根服务器的角色,负责对根区数据的查询进行响应。所有根对等节点通过基于共识的智能合约执行相关操作,如对TLD授权、区域数据发布等。第二层中的节点类似于传统DNS中的除根域以外的其他各级授权服务器,负责对所有存储的域名数据提供相同身份的授权查询。另外,在第二层中FI-DNS通过索引子域数据(index subdomain data),利用区域文件的哈希值实现了域名数据的分级索引,这是因为子域的区域文件的索引信息已经包含在父域的区域文件中。在此情况下,客户端可以通过多次迭代查询获得目标域名的解析数据。

FI-DNS完全继承了传统的DNS名称空间,基于联盟链和智能合约避免了传统DNS系统根区管理过程中存在的单点故障风险。但是,由于FI-DNS实现过程的复杂性,FI-DNS中的解析延时明显高于传统DNS系统,这也是需要进一步研究解决的一个问题。

3.3 小结

与传统DNS一样,以DNSSEC为代表的传统DNS安全增强机制仍然无法阻止DDoS攻击,也无法实现对数据的加密。相反,当域名存储在本地区块链时,用户不需要从远程服务器进行域名查询,因此传统DNS增强中存在的中间人攻击将不会在融入或基于区块链的DNS中发生,同时可有效保护用户的隐私。但是,将区

表4 区块链安全方案分析与比较

Table 4 Analysis and comparison of blockchain security schemes

名称	主要增强方式	区块链技术	共识算法	支持已有 DNS 格式	向后兼 容性	抗 DDoS 攻击	抗缓存区 中毒	域名 劫持	隐私 保护	应用实效
RootChain	根区增强	Hyperledger Fabric	PBFT	✓	✓	仅根区	仅根区	✓	✓	原型系统
Handshake	根区增强	UTXO 模型	PoW	×	✓	仅根区	仅根区	✓	✓	插件、解析器
D ³ NS	根区增强	Bitcoin	PoW	✓	✓	✓	✓	✓	✓	实验验证
IDV	根区增强	联盟链	PBFT	✓	✓	×	✓	✓	✓	原型系统
B-DNSSEC	递归侧增强	—	—	✓	✓	✓	✓	✓	✓	原型系统
TI-DNS	递归侧增强	联盟链	PBFT	×	✓	—	✓	—	—	原型系统
DNS-BC	递归侧增强	联盟链	PBFT	×	✓	✓	✓	✓	✓	原型系统
Namecoin	系统重构	Bitcoin	PoW	✓	×	✓	✓	✓	✓	尚未大规模落地
Blockstack	系统重构	Bitcoin	PoW	✓	×	✓	✓	✓	✓	开源项目
ENS	系统重构	Ethernet	PoS	✓	×	✓	✓	✓	✓	大范围部署
EmerDNS	系统重构	Bitcoin	PoW+PoS	✓	×	✓	✓	✓	✓	小范围应用
B-DNS	系统重构	—	PoS	✓	✓	✓	✓	✓	✓	原型系统
FI-DNS	系统重构	Hyperledger Fabric	PBFT	✓	×	✓	仅根区	✓	—	原型系统

区块链技术应用于对传统 DNS 的增强或构建全新的 DNS 系统,都需要面对以下几个方面的挑战:(1)资源记录的存储问题。一旦将资源记录写入区块链,就很难被修改,但是在实际应用中当域名持有者变更了 IP 地址时就需要更新 DNS 记录,这就需要采用一些新的设计来提供灵活的记录更新。(2)区块链的性能问题。区块链作为 DNS 记录的存储数据库,域名解析过程其实质就是从区块链中查询和验证记录的过程。当对时间敏感的 DNS 查询遇到响应速度较慢的区块链系统时,需要设计一些方案来加快区块链中的记录查询过程。(3)漏洞。将区块链应用于 DNS 后虽然在数据的防篡改和防御 DDoS 攻击方面取得了不错的效果,但区块链固定的安全问题也可能被引入到 DNS 系统,成为新的安全漏洞。为此,如何在不引入新的区块链安全问题的情况下构建融入或基于区块链的 DNS 将面临着很大的挑战。

表 4 围绕所采用的区块链技术类型、采用的共识算法、是否支持已有的 DNS 格式、协议向后兼容性、抵抗 DDoS 攻击、抵抗缓存区中毒、是否存在域名劫持、用户隐私保护以及当前应用现状等方式进行了归纳总结。

4 总结与展望

DNS 提供了域名与 IP 地址两类不同网络标识体系之间的转换机制,是互联网的重要基础设施和流量调度的神经中枢。虽然区块链技术的快速发展为网络安全研究提供了新的思路和实现路径,但受 DNS 技术内生安全和互联网应用复杂性的影响,DNS 安全领域尚有一些问题需要进一步探究。

4.1 总结

安全与应用相伴而生。虽然 DNS 技术随着互联网应用场景的不断丰富而迭代发展,但是 DNS 安全隐患的隐蔽性和攻击行为的不确定性,致使 DNS 安全仍然面临许多风险和挑战。目前,在 DNS 安全领域尚有一些悬而未决的难题,主要表现为:

(1)DNSSEC 的技术实现和部署问题。DNSSEC 通过引入密钥验证机制在数据完整性和来源认证方面提供了基础保障,但其在技术实现和实际部署上仍然存在悬而未决的难题。从技术层面来看,DNSSEC 过于依赖 DNS 的层次结构,基于公钥机制的域名身份注册与绑定在设计上采用中心化方式,DNS 查询路径上的每一个子域必须得到其父域的正确签名,同时域名解析过程中的公钥身份验证必须借助于信任链的验证功能,致使验证过程复杂且密钥管理困难,同时签名验证开销大。从 DNSSEC 部署来看,存在部署的碎片化与信任链断裂问题,而且运维过程复杂。虽然区块链技术的引入解决了一些问题,例如,使用区块链分布式账本存储域名记录以解决中心化数据存储带来的安全风险,再如,由每个节点独立完成信任验证以减小验证过程的复杂性并提升验证的可信性等,但这些方法仍然没有解决 DNSSEC 存在的“安全、性能、易用性”不可能三角问题。

(2)DNS 实时性需求与区块链性能之间的矛盾。衡量一个 DNS 系统性能的一个重要特征是在确保安全的前提下尽可能缩短查询/应答时间,即追求安全、高效的 DNS 查询。然而,现有区块链技术在解决了部分 DNS 安全问题的同时,仍然没有摆脱区块链自身存在的查询延时高、吞吐率低等突出问题的困扰。区块链共

识算法导致查询响应时间远高于传统 DNS, 区块链每秒交易数(transactions per second, TPS)无法支撑日均万亿级的全球 DNS 查询量。为此, 如何在保证去中心化的同时实现 DNS 的快速查询, 虽然目前区块链分片、区块扩容、跨链操作等技术可在一定程度上提高区块链系统的性能, 但与 DNS 查询实时性需求之间存在的差距仍然无法被用户接受。

(3) 智能合约漏洞引发的安全问题。ENS、Handshake、Namecoin 等大量基于区块链的 DNS 安全方案都依赖智能合约管理域名, 然而智能合约一旦部署便难以修改, 使得因安全漏洞导致的后果极为严重。目前, 智能合约中主要存在的数据溢出、访问控制、逻辑错误、时间依赖、预言机操纵、签名重放、短地址攻击等安全漏洞, 都可能导致域名所有权被窃取或域名系统的混乱。为此, 如何形式化验证智能合约的 DNS 业务逻辑, 仍然是一个难题。

(4) 隐私保护与合规性之间的冲突。区块链具有的不可篡改性特征使得所有历史查询记录永久保存在区块链分布式账本中, 其中大量查询信息可能暴露用户的行为模式。在当前用户普遍关注隐私保护、强调“被遗忘权”的情况下, 如何在实现查询验证的前提下有效保护查询内容仍然需要进一步加强研究。另外, 区块链 DNS 可能被用于托管一些非法域名, 而一旦托管将无法被移除, 在此情况下, 如何在技术和法律层面实现域名的监管还需要进行广泛而深入的探讨。

另外, 还存在去中心化治理与命名冲突风险、密钥管理单点故障、与传统 DNS 的兼容性等难题。可以将上述悬而未决的问题概括为去中心化与效率、不可篡改与合规、安全与用户体验 3 类难题。

4.2 展望

区块链提供了有关命名系统的全局状态共识, 并能够为状态改变提供仅可追加的全局日志, 对键/值对的写入只能通过共识过程在新区块中宣布并追加到全局日志中。全局日志实现了逻辑上的集中(网络中的所有节点维护着同一个状态数据)和组织上的分布(没有中央控制机制)。然而, 区块链系统尚处于发展的初期, 区块链技术自身还存在大量影响其普及应用的性能瓶颈和功能限制。未来研究工作可以更多地关注以下几个方面:

(1) DNS 系统去中心化体系结构研究。传统 DNS 系统由 ICANN 中央机构管理, 其运行结构上离不开中心化的分层架构, 其管理模式依赖于基于中央集权的法律框架。中心化体系结构是导致 DNS 系统安全问题难以从根本上解决的主要根源, 利用区块链技术所具有的

去中心化机制来改造或重构 DNS 系统具有重要研究价值和意义^[118-119], 同时主要存在以下两个方面的挑战:

① 区块链自身的性能。目前影响区块链自身性能的主要因素有可扩展性、互操作性、去中心化与监管的冲突、智能合约漏洞等, 这些因素与 DNS 应用场景之间存在着一定的矛盾, 必须有针对性地进行研究。② 共识算法。目前区块链中广泛使用的 PoW、PoS 等共识算法存在分叉现象, 无法保证每个节点存储数据的强一致性, 无法适应 DNS 的应用需求, 为此研究开发符合 DNS 应用场景的更加高效的共识算法是下一步工作的一个重点。

(2) 根服务器和递归解析服务器安全性研究。目前, DNS 安全问题主要来自于根服务器和递归解析服务器, 因此针对根和递归侧的安全研究显得极为重要。DNS 通过由授权服务器组成的全球分布式数据库提供域名服务, 其中共有 13 个由不同利益相关者管理的根 DNS 服务器分别为各自负责的域名提供名字解析服务器。根服务器去中心化是解决当前根中心化管控机制可能引发的对 TLD 管理失控的主要手段, 也是解决根服务器单点失效的途径, 但是如何实现从中心化管制到去中心化协同之间的平滑过渡, 需要同时应对技术和制度层的挑战。DNS 名称解析服务由递归解析器提供本地化服务, 每个客户端主机通过一个称为存根解析器的特殊程序简单地接收来自应用程序(如 Web 浏览器)的 DNS 查询, 并将这些查询转发给递归解析器, 递归解析器随后处理查找并返回结果。利用区块链技术解决递归侧的安全问题是将区块链作为一个可信的分布式资源记录存储平台, 但如何解决域名查询验证过程的效率问题, 以及如何建立关键域名在区块链环境中的安全保全更新机制, 仍然有大量的技术难题需要研究解决。

(3) 兼容性研究。在互联网环境中 DNS 提供的域名解析服务具有基础性和不可替代性, 因此各类 DNS 安全增强方案的提出和部署需要考虑与现有系统之间的兼容性, 尤其是客户端的兼容更能决定一项技术的可行性和生命力。同时还有部署过程的复杂性, DNSSEC 从 1997 年提出到目前为止仍然未能有效在二级域名部署, 就是因为其部署和管理过于复杂, 导致大多数现有 DNS 服务器和客户端不支持 DNSSEC。大量融合区块链技术的 DNS 安全增强技术和基于区块链的 DNS 安全架构被提出, 但大部分方案与现有 DNS 系统之间的兼容性不够友好。因此, 在设计 DNS 安全增强方案和基于区块链的 DNS 安全架构时需要充分考虑与现有 DNS 协议之间的兼容性。

(4) 融入区块链技术的云 DNS 安全研究。DNS 已经从早期简单解决域名与 IP 地址之间的映射关系, 发

展到现在的智能算力和流量调度服务平台,并随着新的功能场景的不断增加,DNS的功能和应用将更加丰富。云服务的灵活性和可伸缩性使其作为一种互联网基础服务设施为构建安全的DNS提供了保障,云DNS将DNS服务托管在云服务提供商的分布式服务器集群上,结合云计算的高可用性、弹性扩展和智能化管理能力,提升解析效率和可靠性。然而,云DNS也存在边缘节点覆盖不足、缓存更新不及时、协议兼容性较差、对复杂网络架构的支持不足及管理复杂等问题。将区块链技术应用于云DNS,一方面可以利用云平台提供的弹性计算资源和分布式存储动态扩展区块链网络的算力和存储空间,提升交易处理速度和数据存储容量,另一方面区块链为云DNS提供了去中心化信任和抗审查能力。为此,如何将云计算与区块链相结合,构建更加安全、高效、可信和可有效保护用户隐私的DNS服务,还需要在融合各技术的基础上结合DNS安全问题进行深入研究。

综上,将区块链技术用于解决传统DNS中存在的安全问题或重构一个全新的域名系统,无论是理论研究还是现实需求都是一项很有必要且极具价值的工作。与互联网时代相比,区块链是一种很有发展前途的新技术,它通过网络中互不信任的节点支持着一种去中心化的新型信任机制,基于或融入区块链的DNS系统正是由这一信任机制支撑的产物。然而,在这一技术被互联网完全采用之前仍然存在一些挑战和悬而未决问题,这些都是下一步亟待研究和解决的关键问题。

参考文献:

- [1] MOCKAPETRIS P. Domain names - concepts and facilities: RFC1034[S/OL]. (1983-11-01) [2024-08-23]. <https://www.rfc-editor.org/rfc/pdf/rfc1034.txt.pdf>.
- [2] JAIN K, JAIN M, BORADE J L. A survey on man in the middle attack[J]. International Journal for Science Technology and Engineering, 2016, 2: 277-280.
- [3] ALIEYAN K, KADHUM M M, ANBAR M, et al. An overview of DDoS attacks based on DNS[C]//Proceedings of the 2016 International Conference on Information and Communication Technology Convergence. Piscataway: IEEE, 2016: 276-280.
- [4] KIM T H, REEVES D. A survey of domain name system vulnerabilities and attacks[J]. Journal of Surveillance, Security and Safety, 2020, 1(1): 34-60.
- [5] HERZBERG A, SHULMAN H. DNSSEC: security and availability challenges[C]//Proceedings of the 2013 IEEE Conference on Communications and Network Security. Piscataway: IEEE, 2013: 365-366.
- [6] VAN RIJSWIJK-DEIJ R, SPEROTTO A, PRAS A. DNS-SEC and its potential for DDoS attacks: a comprehensive measurement study[C]//Proceedings of the 2014 Conference on Internet Measurement Conference. New York: ACM, 2014: 449-460.
- [7] AFEK Y, BREMLER-BARR A, SHAFIR L. NXNSAttack: recursive DNS inefficiencies and vulnerabilities[EB/OL]. [2024-08-26]. <https://arxiv.org/abs/2005.09107>.
- [8] NADLER A, BITTON R, BRODT O, et al. On the vulnerability of anti-malware solutions to DNS attacks[J]. Computers & Security, 2022, 116: 102687.
- [9] CHIJOKE AHAKONYE L A, IFEANYI NWAKANMA C, AJAKWE S O, et al. Countering DNS vulnerability to attacks using ensemble learning[C]//Proceedings of the 2022 International Conference on Artificial Intelligence in Information and Communication. Piscataway: IEEE, 2022: 7-10.
- [10] ASLAN Ö, AKTUĞ S S, OZKAN-OKAY M, et al. A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions[J]. Electronics, 2023, 12(6): 1333.
- [11] BENOMAR Z, LONGO F, MERLINO G, et al. A cloud-based and dynamic DNS approach to enable the web of things [J]. IEEE Transactions on Network Science and Engineering, 2022, 9(6): 3968-3978.
- [12] SALAT L, DAVIS M, KHAN N. DNS tunnelling, exfiltration and detection over cloud environments[J]. Sensors, 2023, 23(5): 2760.
- [13] SCHMID G. Thirty years of DNS insecurity: current issues and perspectives[J]. IEEE Communications Surveys & Tutorials, 2021, 23(4): 2429-2459.
- [14] LYU M Z, GHARAKHEILI H H, SIVARAMAN V. A survey on DNS encryption: current development, malware misuse, and inference techniques[J]. ACM Computing Surveys, 2023, 55(8): 1-28.
- [15] AL-MASHHADI S, MANICKAM S. A brief review of blockchain-based DNS systems[J]. International Journal of Internet Technology and Secured Transactions, 2020, 10(4): 420.
- [16] 王文通, 胡宁, 刘波, 等. DNS安全防护技术研究综述[J]. 软件学报, 2020, 31(7): 2205-2220.
WANG W T, HU N, LIU B, et al. Survey on technology of security enhancement for DNS[J]. Journal of Software, 2020, 31(7): 2205-2220.
- [17] 张宾, 张宇, 张伟哲. 递归侧DNS安全研究与分析[J]. 软件学报, 2024, 35(10): 4876-4911.
ZHANG B, ZHANG Y, ZHANG W Z. Study and analysis of recursive side DNS security[J]. Journal of Software, 2024, 35(10): 4876-4911.

- [18] 夏玲玲, 王群, 马卓, 等. 区块链在 PKI 安全中的应用研究[J]. 计算机科学与探索, 2024, 18(10): 2573-2593.
- XIA L L, WANG Q, MA Z, et al. Research on application of blockchain in PKI security[J]. Journal of Frontiers of Computer Science and Technology, 2024, 18(10): 2573-2593.
- [19] ZOU F T, ZHANG S Y, PEI B, et al. Survey on domain name system security[C]//Proceedings of the 2016 IEEE 1st International Conference on Data Science in Cyberspace. Piscataway: IEEE, 2016: 602-607.
- [20] ALHARBI F, ZHOU Y C, QIAN F, et al. DNS poisoning of operating system caches: attacks and mitigations[J]. IEEE Transactions on Dependable and Secure Computing, 2022, 19(4): 2851-2863.
- [21] VON ARX K G, HAGAN G R. Sovereign domains: a declaration of independence of ccTLDs from foreign control[J]. Richmond Journal of Law and Technology, 2002, 9: 4.
- [22] IANA. Root servers[EB/OL]. [2024-08-18]. <https://www.iana.org/domains/root/servers>.
- [23] SCHOMP K, CALLAHAN T, RABINOVICH M, et al. Assessing DNS vulnerability to record injection[C]//Proceedings of the 2014 International Conference on Passive and Active Network Measurement. Cham: Springer, 2014: 214-223.
- [24] DECCIO C, DAVIS J. DNS privacy in practice and preparation[C]//Proceedings of the 15th International Conference on Emerging Networking Experiments and Technologies. New York: ACM, 2019: 138-143.
- [25] IMANA B, KOROLOVA A, HEIDEMANN J. Institutional privacy risks in sharing DNS data[C]//Proceedings of the 2021 Applied Networking Research Workshop. New York: ACM, 2021: 69-75.
- [26] WICINSKI T. DNS privacy considerations: RFC9076[S/OL]. (2021-07-01) [2024-08-17]. <https://www.rfc-editor.org/rfc/rfc9076.pdf>.
- [27] Internet Systems Consortium. Domain server software distribution[EB/OL]. (2019-01-01) [2024-08-26]. <https://ftp.isc.org/www/survey/reports/2019/01/fpdns.txt>.
- [28] AHMAD R, ALSMADI I, ALHAMDANI W, et al. Zero-day attack detection: a systematic literature review[J]. Artificial Intelligence Review, 2023, 56(10): 10733-10811.
- [29] 互联网域名系统国家工程研究中心(ZDNS). 网络安全宣传周: 2024 年 10 大 DNS 安全事件, 影响范围波及全球[EB/OL]. (2024-09-10) [2024-09-15]. <https://www.zdns.cn/h-nd-532.html>.
- Internet Domain Name System National Engineering Research Center(ZDNS). China cybersecurity week: the top 10 DNS security incidents in 2024 have a global impact[EB/OL]. (2024-09-10) [2024-09-15]. <https://www.zdns.cn/h-nd-532.html>.
- [30] CHEN L G, ZHANG Y D, ZHAO Q, et al. Detection of DNS DDoS attacks with random forest algorithm on spark[J]. Procedia Computer Science, 2018, 134: 310-315.
- [31] TREJO L A, FERMAN V, MEDINA-PÉREZ M A, et al. DNS-ADVP: a machine learning anomaly detection and visual platform to protect top-level domain name servers against DDoS attacks[J]. IEEE Access, 2019, 7: 116358-116369.
- [32] MAKSTUTOV A A, CHEREPANOV I A, ALEKSEEV M S. Detection and prevention of DNS spoofing attacks[C]//Proceedings of the 2017 Siberian Symposium on Data Science and Engineering. Piscataway: IEEE, 2017: 84-87.
- [33] CHENG Y N, LIU Y L, LI C, et al. In-depth evaluation of the impact of national-level DNS filtering on DNS resolvers over space and time[J]. Electronics, 2022, 11(8): 1276.
- [34] JACKSON C, BARTH A, BORTZ A, et al. Protecting browsers from DNS rebinding attacks[J]. ACM Transactions on the Web, 2009, 3(1): 1-26.
- [35] HOUSER R, HAO S, LI Z, et al. A comprehensive measurement-based investigation of DNS hijacking[C]//Proceedings of the 2021 40th International Symposium on Reliable Distributed Systems. Piscataway: IEEE, 2021: 210-221.
- [36] JERABEK K, HYNEK K, RYSAVY O, et al. DNS over HTTPS detection using standard flow telemetry[J]. IEEE Access, 2023, 11: 50000-50012.
- [37] MAN K Y, QIAN Z Y, WANG Z J, et al. DNS cache poisoning attack reloaded: revolutions with side channels[C]//Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security. New York: ACM, 2020: 1337-1350.
- [38] SOLIMAN A K, SALAMA C, MOHAMED H K. Detecting DNS reflection amplification DDoS attack originating from the cloud[C]//Proceedings of the 2018 13th International Conference on Computer Engineering and Systems. Piscataway: IEEE, 2018: 145-150.
- [39] XU K, BUTLER P, SAHA S, et al. DNS for massive-scale command and control[J]. IEEE Transactions on Dependable and Secure Computing, 2013, 10(3): 143-153.
- [40] AL MESSABI K, ALDWAIRI M, AL YOUSIF A, et al. Malware detection using DNS records and domain name features[C]//Proceedings of the 2nd International Conference on Future Networks and Distributed Systems. New York: ACM, 2018: 1-7.
- [41] RAVI V, ALAZAB M, SRINIVASAN S, et al. Adversarial defense: DGA-based botnets and DNS homographs detection through integrated deep learning[J]. IEEE Transactions on Engineering Management, 2023, 70(1): 249-266.
- [42] WANG Y, ZHOU A M, LIAO S, et al. A comprehensive sur-

- vey on DNS tunnel detection[J]. Computer Networks, 2021, 197: 108322.
- [43] MOURA G C M, CASTRO S, HEIDEMANN J, et al. Tsunami: exploiting misconfiguration and vulnerability to DDoS DNS[C]//Proceedings of the 21st ACM Internet Measurement Conference. New York: ACM, 2021: 398-418.
- [44] JEITNER P, SHULMAN H, WAIDNER M. The impact of DNS insecurity on time[C]//Proceedings of the 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks. Piscataway: IEEE, 2020: 266-277.
- [45] 喻波, 苏金树, 杨强, 等. 网络协议软件漏洞挖掘技术综述[J]. 软件学报, 2024, 35(2): 872-898.
- YU B, SU J S, YANG Q, et al. Survey on vulnerability mining techniques of network protocol software[J]. Journal of Software, 2024, 35(2): 872-898.
- [46] Squish. DNS traversal checker[EB/OL]. [2024-09-20]. <http://dns.squish.net/>.
- [47] KAKARLA S K R, BECKETT R, ARZANI B, et al. Groot: proactive verification of DNS configurations[C]//Proceedings of the Annual Conference of the ACM Special Interest Group on Data Communication on the Applications, Technologies, Architectures, and Protocols for Computer Communication. New York: ACM, 2020: 310-328.
- [48] ZHANG H K, YE J Y, HU W H, et al. Study on the latent state of Kaminsky-style DNS cache poisoning: modeling and empirical analysis[J]. Computers & Security, 2021, 110: 102445.
- [49] AKKERHUIS J, CHAPIN L, FALTSTROM P, et al. Report on the impact on the DNS root system of increasing the size and volatility of the root zone[EB/OL]. (2009-09-20) [2024-09-20]. <https://www.icann.org/en/system/files/files/root-scaling-study-report-31aug09-en.pdf>.
- [50] GIJSEN B, JAMAKOVIC A, ROIJERS F. Root scaling study: description of the DNS root scaling model[EB/OL]. (2009-09-29) [2024-09-20]. <https://www.icann.org/en/system/files/files/root-scaling-model-description-29sep09-en.pdf>.
- [51] ARENDS R, AUSTEIN R, LARSON M, et al. Protocol modifications for the DNS security extensions: RFC4035[S]. 2005.
- [52] DICKINSON J, DICKINSON S, BELLIS R, et al. DNS transport over TCP-implementation requirements: IETF RFC5966[S]. 2016.
- [53] DAMAS J, GRAFF M, VIXIE P. Extension mechanisms for DNS (EDNS(0)): IETF RFC6891[S]. 2013.
- [54] FOX G. Peer-to-peer networks[J]. Computing in Science & Engineering, 2001, 3(3): 75-77.
- [55] COX R, MUTHITACHAROEN A, MORRIS R T. Serving DNS using a peer-to-peer lookup service[C]//Proceedings of the 1st International Workshop on Peer-to-Peer Systems. Berlin, Heidelberg: Springer, 2002: 155-165.
- [56] QIAN T, MUELLER F, XIN Y F. A real-time distributed hash table[C]//Proceedings of the 2014 IEEE 20th International Conference on Embedded and Real-Time Computing Systems and Applications. Piscataway: IEEE, 2014: 1-10.
- [57] GitHub. dhash[EB/OL]. [2024-10-10]. https://gitcode.com/gh_mirrors/dh/dhash/overview.
- [58] STOICA I, MORRIS R, LIBEN-NOWELL D, et al. Chord: a scalable peer-to-peer lookup protocol for Internet applications[J]. IEEE/ACM Transactions on Networking, 2003, 11(1): 17-32.
- [59] DANIELIS P, ALTMANN V, SKODZIK J, et al. P-DONAS[J]. ACM Transactions on Internet Technology, 2015, 15(3): 1-21.
- [60] MAYMOUNKOV P, MAZIÈRES D. Kademia: a peer-to-peer information system based on the XOR metric[C]//Proceedings of the 1st International Workshop on Peer-to-Peer Systems. Berlin, Heidelberg: Springer, 2002: 53-65.
- [61] RAMASUBRAMANIAN V, SIRER E G. The design and implementation of a next generation name service for the Internet[J]. ACM SIGCOMM Computer Communication Review, 2004, 34(4): 331-342.
- [62] RAMASUBRAMANIAN V, SIRER E G. Beehive: exploiting power law query distributions for O(1) lookup performance in peer to peer overlays[C]//Proceedings of the 1st Conference on Networked Systems Design and Implementation. Berkeley: USENIX Association, 2004: 1-14.
- [63] SANCHO R, PEREIRA R L. Hybrid peer-to-peer DNS[C]//Proceedings of the 2014 International Conference on Computing, Networking and Communications. Piscataway: IEEE, 2014: 977-981.
- [64] HOFFMAN P E. DNS security extensions (DNSSEC): RFC9364[S/OL]. (2023-02-01) [2025-02-03]. <https://www.hjp.at/doc/rfc/rfc9364.html>.
- [65] ATENIESE G, MANGARD S. A new approach to DNS security (DNSSEC)[C]//Proceedings of the 8th ACM Conference on Computer and Communications Security. New York: ACM, 2001: 86-95.
- [66] ARENDS R, AUSTEIN R, LARSON M, et al. DNS security introduction and requirements: RFC4033[S/OL]. (2005-03-01) [2025-02-05]. <https://datatracker.ietf.org/doc/rfc4033/>.
- [67] SURY O, EDMONDS R. Edwards-curve digital security algorithm (EdDSA) for DNSSEC: RFC8080[S/OL]. (2017-02-01) [2025-02-06]. <https://www.rfc-editor.org/info/rfc8080>.
- [68] FUJIWARA K, KATO A, KUMARI W. Aggressive use of DNSSEC-validated cache: RFC8198[S/OL]. (2017-07-01)

- [2025-02-06]. <https://www.rfc-editor.org/info/rfc8198>.
- [69] HOFFMAN P. Revised IANA considerations for DNSSEC: RFC9157[S/OL]. (2021-12-01) [2025-02-06]. <https://www.rfc-editor.org/info/rfc9157>.
- [70] DEMPSKY M. DNSCurve: link-level security for the domain name system draft-dempsey-dnscurve-01[EB/OL]. (2010-02-27) [2025-02-06]. <https://datatracker.ietf.org/doc/html/draft-dempsey-dnscurve>.
- [71] DNSCurve: usable security for DNS[EB/OL]. [2025-02-07]. <https://www.dnscurve.org/index.html>.
- [72] DENIS F. The DNSCrypt protocol draft-denis-dprive-dnscrypt-05[EB/OL]. (2025-01-30) [2025-02-07]. <https://datatracker.ietf.org/doc/draft-denis-dprive-dnscrypt/>.
- [73] PARK S, PAI V S, PETERSON L L, et al. CoDNS: improving DNS performance and reliability via cooperative lookups [C]//Proceedings of the 6th Symposium on Operating Systems Design and Implementation. Berkeley: USENIX Association, 2004: 14.
- [74] CoDNS: making DNS lookups faster, more reliable, and more predictable[EB/OL]. [2025-02-07]. <https://codeen.cs.princeton.edu/codns/>.
- [75] POOLE L, PAI V S. Confidns: leveraging scale and history to improve DNS security[C]//Proceedings of the 3rd Conference on USENIX Workshop on Real, Large Distributed Systems, 2006: 3.
- [76] ZHU L, HU Z, HEIDEMANN J, et al. T-DNS: connection-oriented DNS to improve privacy and security[C]//Proceedings of the 2014 ACM SIGCOMM 2014 Conference. New York: ACM, 2014: 379-380.
- [77] CHHABRA R, MURLEY P, KUMAR D, et al. Measuring DNS-over-HTTPS performance around the world[C]//Proceedings of the 21st ACM Internet Measurement Conference. New York: ACM, 2021: 351-365.
- [78] KOSHY A M, YELLUR G, KAMMACHI H J, et al. An insight into encrypted DNS protocol: DNS over TLS[C]//Proceedings of the 2021 4th International Conference on Recent Developments in Control, Automation & Power Engineering. Piscataway: IEEE, 2021: 379-383.
- [79] KHURSHID A, KIYAK F, CAESAR M. Improving robustness of DNS to software vulnerabilities[C]//Proceedings of the 27th Annual Computer Security Applications Conference. New York: ACM, 2011: 177-186.
- [80] SCAIFE N, CARTER H, LIDSKY L, et al. OnionDNS: a seizure-resistant top-level domain[J]. International Journal of Information Security, 2018, 17: 645-660.
- [81] 王群, 李馥娟, 王振力, 等. 区块链原理及关键技术[J]. 计算机科学与探索, 2020, 14(10): 1621-1643.
- WANG Q, LI F J, WANG Z L, et al. Principle and core technology of blockchain[J]. Journal of Frontiers of Computer Science and Technology, 2020, 14(10): 1621-1643.
- [82] ZHANG Y, LIU W F, XIA Z D, et al. Blockchain-based DNS root zone management decentralization for Internet of things[J]. Wireless Communications and Mobile Computing, 2021(1): 6620236.
- [83] LIU Y, YU H S, WANG W Y, et al. A robust blockchain-based distribution master for distributing root zone data in DNS[J]. The Computer Journal, 2022, 65(11): 2880-2893.
- [84] HE G B, SU W, GAO S, et al. TD-Root: a trustworthy decentralized DNS root management architecture based on permissioned blockchain[J]. Future Generation Computer Systems, 2020, 102: 912-924.
- [85] Handshake[EB/OL]. [2025-02-18]. <https://handshake.org/>.
- [86] BENSHOOF B, ROSEN A, BOURGEOIS A G, et al. Distributed decentralized domain name service[C]//Proceedings of the 2016 IEEE International Parallel and Distributed Processing Symposium Workshops. Piscataway: IEEE, 2016: 1279-1287.
- [87] UrDHT[EB/OL]. [2025-03-07]. <https://github.com/UrDHT>.
- [88] HU N, TENG Y, ZHAO Y, et al. IDV: Internet domain name verification based on blockchain[J]. Computer Modeling in Engineering & Sciences, 2021, 129(1): 299-322.
- [89] ZOLFAGHARI B, SRIVASTAVA G, ROY S, et al. Content delivery networks[J]. ACM Computing Surveys, 2021, 53(2): 1-34.
- [90] GOURLEY S, TEWARI H. Blockchain backed DNSSEC[C]//Proceedings of the 2018 International Conference on Business Information Systems. Cham: Springer, 2018: 173-184.
- [91] Sun Microsystems, Inc. Public key infrastructure overview [EB/OL]. (2001-08-01) [2025-03-10]. http://highsecu.free.fr/db/outils_de_securite/cryptographie/pki/publickey.pdf.
- [92] TEWARI H, HUGHES A, WEBER S, et al. X509Cloud: framework for a ubiquitous PKI[C]//Proceedings of the 2017 IEEE Military Communications Conference. Piscataway: IEEE, 2017: 225-230.
- [93] FU Y F, WEI J Q, LI Y, et al. TI-DNS: a trusted and incentive DNS resolution architecture based on blockchain[C]//Proceedings of the 2023 IEEE 22nd International Conference on Trust, Security and Privacy in Computing and Communications. Piscataway: IEEE, 2023: 265-274.
- [94] YU Z, XUE D, FAN J L, et al. DNSTSM: DNS cache resources trusted sharing model based on consortium blockchain[J]. IEEE Access, 2020, 8: 13640-13650.
- [95] GAO T F, DONG Q K. DNS-BC: fast, reliable and secure domain name system caching system based on a consor-

- tium blockchain[J]. Sensors, 2023, 23(14): 6366.
- [96] KCP-a fast and reliable ARQ protocol[EB/OL]. [2025-03-02]. <https://github.com/skywind3000/kcp>.
- [97] CHEN W Y, YANG X, ZHANG H K, et al. Big data architecture for scalable and trustful DNS based on sharded DAG blockchain[J]. Journal of Signal Processing Systems, 2021, 93(7): 753-768.
- [98] DIGITALE J C, MARTIN J N, GLYMOUR M M. Tutorial on directed acyclic graphs[J]. Journal of Clinical Epidemiology, 2022, 142: 264-267.
- [99] Namecoin[EB/OL]. [2025-03-02]. <https://www.namecoin.org/>.
- [100] ncdns[EB/OL]. [2025-03-06]. <https://www.namecoin.org/docs/ncdns/>.
- [101] BOER T D, BREIDER V. Invisible Internet project (I2P) [EB/OL]. (2019-02-10) [2025-03-02]. <https://rp.os3.nl/2018-2019/p63/report.pdf>.
- [102] KALODNER H A, CARLSTEN M, ELLENBOGEN P, et al. An empirical study of namecoin and lessons for decentralized namespace design[J]. Journal of Cybersecurity, 2015, 1(1): 1-23.
- [103] ALI M, NELSON J, SHEA R, et al. Blockstack: a global naming and storage system secured by blockchains[C]// Proceedings of the 2016 USENIX Annual Technical Conference. Berkeley: USENIX Association, 2016: 181-194.
- [104] Access handshake names[EB/OL]. [2025-03-09]. <https://learn.namebase.io/starting-from-zero/how-to-access-handshake-sites>.
- [105] ENS[EB/OL]. [2025-03-09]. <https://ens.domains/>.
- [106] TAHERDOOST H. Non-fungible tokens (NFT): a systematic review[J]. Information, 2023, 14(1): 26.
- [107] ENSv2: the next generation of ENS[EB/OL]. (2024-05-28) [2025-03-11]. <https://ens.domains/blog/post/ensv2>.
- [108] DIB O, TOUMI K. Decentralized identity systems: architecture, challenges, solutions and future directions[J]. Annals of Emerging Technologies in Computing, 2020, 4(5): 19-40.
- [109] EmerDNS[EB/OL]. [2025-03-18]. <https://emercoin.com/en/emerdns/>.
- [110] Emercoin blockchain[EB/OL]. [2025-03-18]. <https://emercoin.com/en/>.
- [111] OpenNIC[EB/OL]. [2025-03-20]. <https://github.com/OpenNIC>.
- [112] ipfs[EB/OL]. [2025-03-20]. <https://github.com/ipfs/ipfs>.
- [113] CASINO F, LYKOUSAS N, KATOS V, et al. Unearthing malicious campaigns and actors from the blockchain DNS ecosystem[J]. Computer Communications, 2021, 179: 217-230.
- [114] LI Z C, GAO S, PENG Z, et al. B-DNS: a secure and efficient DNS based on the blockchain technology[J]. IEEE Transactions on Network Science and Engineering, 2021, 8(2): 1674-1686.
- [115] PeerName[EB/OL]. [2025-03-22]. <https://peername.com/>.
- [116] JIN L, HAO S, HUANG Y, et al. DNSonChain: delegating privacy-preserved DNS resolution to blockchain[C]// Proceedings of the 2021 IEEE 29th International Conference on Network Protocols. Piscataway: IEEE, 2021: 1-11.
- [117] LIU W F, ZHANG Y, LIU L, et al. A secure domain name resolution and management architecture based on blockchain[C]// Proceedings of the 2020 IEEE Symposium on Computers and Communications. Piscataway: IEEE, 2020: 1-7.
- [118] KOVALENKO Y. Web3 domain dispute resolution framework (v1.0)[EB/OL]. (2025-03-19) [2025-03-26]. <https://ssrn.com/abstract=5185473>.
- [119] KOCAOGULLAR Y, OSTERWEIL E, ZHANG L. Towards a decentralized Internet namespace[C]// Proceedings of the 2024 Workshop on the Decentralization of the Internet. New York: ACM, 2024: 36-41.



倪雪莉 (1990—), 女, 江苏南通人, 博士研究生, 副教授, CCF 会员, 主要研究方向为区块链技术及应用、网络空间安全。

NI Xueli, born in 1990, Ph.D. candidate, associate professor, CCF member. Her research interests include blockchain technology and applications, cyberspace security.



王群 (1971—), 男, 甘肃天水人, 博士, 教授, CCF 杰出会员, 主要研究方向为信息安全、计算机网络体系结构与协议。

WANG Qun, born in 1971, Ph.D., professor, CCF distinguished member. His research interests include information security, computer network architecture and protocols.



马卓 (1993—), 女, 山西太原人, 博士, 讲师, CCF 会员, 主要研究方向为网络空间安全。

MA Zhuo, born in 1993, Ph.D., lecturer, CCF member. Her research interest is cyberspace security.