

互联网 DNS 安全研究现状与挑战

胡宁¹, 邓文平¹, 姚苏²

(1. 国防科技大学计算机学院, 湖南 长沙 410073;

2. 北京交通大学电子信息工程学院, 北京 100044)

摘要: 域名系统为互联网的应用提供域名与 IP 地址的相互转换服务, 是互联网的重要基础设施。DNS 的安全是互联网稳定运行的保障, 也是互联网安全研究的重要内容。现有研究主要通过设计增强协议、监测机制和使用方法来提高 DNS 系统的安全防护能力, 但近期的 DNS 攻击事件表明, DNS 安全依然存在很多极具挑战性的问题没有解决。从安全增强、行为监测和隐私保护等方面对现有成果和挑战问题进行了总结和讨论。

关键词: DNS 安全; DNS 监测; DNS 隐私保护; 互联网安全

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00154

Issues and challenges of Internet DNS security

HU Ning¹, DENG Wen-ping¹, YAO Su²

(1. School of Computer, National University of Defense Technology, Changsha 410073, China;

2. School of Electronics and Information Engineering, Beijing Jiaotong University, Beijing 100044, China)

Abstract: The domain name system is a critical component of the Internet infrastructure, which maps host names to IP addresses and is involved in most Internet transactions. DNS security has a profound effect on the overall security of Internet and it is also a vital research content of Internet security. In order to improve the security capability of DNS, many enhanced protocols, monitoring mechanisms and best practices were proposed. But recent DNS attack events indicate there are still many recent major research challenges of DNS security problems. The existing achievements and challenges were summarized and discussed, which included security enhanced, behavior monitoring and privacy protection.

Key words: DNS security, DNS monitor, DNS privacy reserve, Internet security

1 引言

域名系统 (DNS, domain name system) 是互联网的重要基础设施, 是联接互联网各类应用与资源的纽带, 为各种基于域名的 Web 应用、电子邮件和分布式系统的正常运行提供关键性支撑服务。目前, 全球域名总数超过 3 亿, 域名服务器

数量超过 1 000 万台, 每天提供千亿次的查询服务。因此, DNS 系统的安全对互联网的正常运行举足轻重。随着互联网商业价值的提升, 恶意攻击者开始利用 DNS 系统实施网络攻击, 一些大型恶意组织甚至可以利用他们特有的能力构造攻击行为, 对互联网整体的运行造成严重的影响^[1]。为了提高 DNS 系统的安全防护能力, 涌现了大量

收稿日期: 2016-12-15; 修回日期: 2017-01-28。通信作者: 胡宁, huning@nudt.edu.cn

基金项目: 国家自然科学基金资助项目 (No.61202486)

Foundation Item: The National Natural Science Foundation of China (No.61202486)

优秀的研究成果^[2],但随着计算机技术的不断发展以及互联网应用模式的不断变化,DNS系统依然面临许多安全威胁和技术挑战^[3,4]。

DNS系统最早于1983年由Mockapetris提出,其主要功能是解决域名与地址转换的问题^[5]。经典的DNS系统包括域名空间和资源记录、域名服务器和域名解析器。域名服务器提供域名空间和资源记录的存储和访问服务,也称为服务基础设施。域名解析器负责接收客户端请求并查询域名服务器,也称为客户基础设施。DNS的工作原理非常简单,以域名www.example.com为例,首先是应用程序通过操作系统的接口向域名解析器发出解析请求,域名解析器收到请求后,从根服务器查询到能够解析“.com”的名字服务器,然后从该服务器查询到能够解析“example.com”的名字服务器,再从“example.com”的名字服务器查询能够解析“www.example.com”的服务器,依次类推,最后能够解析“www.example.com”的服务器查询与“www.example.com”对应的IP地址。上述查询过程中产生的结果,在域名解析器本地缓存,为后续的查询提高效率。

DNS系统的主要工作机制和协议规范在IETF的RFC1034和RFC1035已经基本成熟,随着其应用环境的不断变化以及互联网自身的发展,DNS的相关规范也在不断完善,截至2015年11月,与DNS直接相关的RFC规范达到182条^[6]。互联网DNS系统已经从一个简单的查询系统,发展成一个复杂的生态系统^[7]。随着DNS被赋予更多的应用功能支持,如负载均衡、缓冲、流量工程等^[8,9],上述这个简单的过程变得非常复杂,尤其当该过程被恶意用户利用时,将会产生严重的DNS安全事件。事实上,近年来,发生的多起DNS安全事件,已经广泛引起了业界的重视^[10-13],DNS的安全问题并没有得到完善的解决,依然存在一些挑战和开放性课题。

为了更好地理解DNS安全问题的本质,把握研究热点和方向,本文从脆弱分析、安全增强、诊断监控和隐私保护等方面,对近年来关于DNS安全的多篇学术论文进行了归纳分析,并在此基础上,对今后的研究方向和挑战问题

进行了预测。

2 研究现状

2.1 脆弱分析

DNS系统在最初被提出时,在协议设计和系统实现等方面没有过多考虑安全机制。虽然DNS系统的工作原理比较简单,但是实际运行过程中,却表现出很高的复杂性,造成这种复杂性的主要原因包括用户行为、系统结构、缓冲机制等。DNS系统的这种复杂性为安全防护带来了障碍。RFC 3833将DNS系统的安全威胁分为3个方面:1)服务器与解析器之间的安全通信威胁;2)利用已有服务构造拒绝服务攻击(DoS/DDoS);3)利用软件实现上存在的漏洞或者错误控制提升权限,控制DNS服务器^[14]。文献[15]认为DNS系统的安全威胁主要包括数据威胁、协议威胁、系统威胁和网络威胁。文献[16]将DNS系统面临的安全威胁分为拒绝服务攻击、数据虚假、信息泄露。

DNS系统之所以面临上述安全威胁,其根本是因为协议脆弱性和系统脆弱性。

2.1.1 协议脆弱性

DNS系统的脆弱性来自DNS协议自身。传统的DNS系统基于UDP交换DNS消息,在消息交换的过程中,所有请求消息和应答消息都采用明文传递,资源记录不提供数字签名等防伪造保护。这类协议很容易受到中间人攻击,通过窃听、篡改和伪造DNS消息的方式对DNS系统进行攻击。

文献[17]评估DNS系统在抵御DNS记录注入攻击时的脆弱性,发现利用缓冲区投毒实现DNS伪造记录注入的现象是非常普遍的。当前互联网有大量免费DNS解析器存在,为恶意攻击者提供了更多的攻击目标,实验结果表明,有7%~9%的解析器容易受到注入攻击^[18]。文献[19]展示了“流氓”DNS服务器如何通过构造虚假的DNS解析路径,导致用户请求被发送到恶意的DNS名字服务器上。文献[20]利用校园网数据和从alexa.com获得的10⁶个域名,对一些恶意DNS的行为进行了定量分析,实验结果证明,使用域名服务作为隐形僵尸网络命令和控制通道的可行性是非常大的。

DNS 协议在安全防护方面的不足,还导致了用户隐私泄露问题。随着互联网商业价值的不断提升,用户隐私问题成为 DNS 系统面临的一个重要问题^[21,22]。由于 DNS 的查询携带了足够的信息,用户应用在通过 DNS 解析域名的过程中,可能会泄露用户兴趣爱好、身份信息和设备类型等隐私信息,一些公司通过收集用户的 DNS 信息流来分析用户行为,并为此设计商业行为。文献[23]对这类安全威胁进行了分析。文献[24]通过校园网收集 DNS 的公告数据集,发现存在大量的隐私泄露风险,如用户真实姓名、设备名称等。文献[25]讨论了 DNS 预解析和隐私泄露的矛盾。很多浏览器为了优化浏览性能,往往会对网页中包含的域名进行预解析,这种做法可能会导致隐私威胁或被攻击者滥用。文献[26]在真实环境下,对基于流量的行为跟踪技术进行了可行性分析,提出一种基于朴素贝叶斯模型的行为分类器,结合 DNS 日志对用户行为进行分析,实验结果表明,通过 DNS 的请求来分析用户行为的准确度可以达到 88%,这说明恶意攻击者是完全有可能通过分析用户的 DNS 请求序列来分析用户的隐私,同时也说明现有的 DNS 协议在保护用户隐私方面存在缺陷。

2.1.2 系统脆弱性

DNS 系统的脆弱性来自 DNS 系统的组成与实现方式。DNS 系统经过多年的发展,已经成为一个复杂的生态系统,包含了大量开放的 DNS 服务提供商^[27],这些解析器有些是可信任的,有些则是半可信任甚至不可信任的。一次看似简单的域名解析过程,很可能会涉及多台位于多个不同层级、不同地域的域名服务器和解析器^[28],形成一条复杂的解析路径,而构成解析路径的各个节点之间并没有建立起有效的信任传递关系。

文献[29]对互联网的 DNS 解析器进行了探测,探测结果表明在当前互联网环境下,至少存在 $15 \times 10^6 \sim 32 \times 10^6$ 个开放式 DNS 解析器,这些解析器可以分为 3 类: 1) 专门负责接收用户的解析请求; 2) 负责与域名服务器交互,返回解析结果; 3) 前 2 类解析的中间人,负责转发各种解析请求。其中,后 2 类解析器对终端用户并不可见,并且这些开放式解析器的管理和实现都存在不规

范的现象,以 TTL 设置为例,只有 19% 的解析器能够返回正确的 TTL,其他一些研究成果也发现了类似现象^[30,31]。

文献[32]研究对 DNS 系统的域名服务器进行了拓扑分析,发现在名字服务器之前,存在大量用户无法直接访问到的解析器,这些解析器起到 Cache 的作用,能够将历史的解析结果缓存起来,以便提高解析结果。由于这些解析器大多由第三方机构管理,在部署和配置管理方面,没有遵守最佳实践原则,如 RFC5452、RFC4697,因此存在许多安全隐患。

2.2 安全增强

对 DNS 系统自身进行安全增强的研究成果主要包括: 对 DNS 协议的安全扩充和对 DNS 系统的实现进行增强 2 个方面。

2.2.1 DNS 协议增强

传统 DNS 协议安全的不足在于对信息缺乏真实性和保密性的保护,为了防止缓冲区投毒攻击,DNSSEC 和 NSEC3 被引入 DNS 体系,DNSEC^[33]是迄今最为著名的 DNS 安全增强方案,以公钥密码机制为基础,为 DNS 的资源记录计算数字签名,通过验证数字签名来确保解析结果的真实性。DNSEC 在 DNS 的基础上,扩展了一些重要的安全记录,包括以下内容。1) DNSKEY 记录,用于记录域名服务器的公开密钥。2) RRSIG 记录,用于存储对资源记录集合 (RRSet) 计算的数字签名。3) DS 记录,存储 DNSKEY 的散列值,用于验证 DNSKEY 的真实性,DS 记录存储在上级域名服务器,因此,在验证某域名服务器数字证书的真实性时,需要从上一级域名服务器获取其 DS 记录,这样就形成了逐级认证的信任链。4) NSEC 记录,用于表示请求的域名不存在。DNSSEC 在解析域名时,包括 2 个过程。一个是域名解析过程,与 DNS 解析过程一致,但域名解析的应答结果中,除了包含资源记录 (RR),还同时包含域名服务器对资源记录的数字签名 (RRSIG); 另外一个过程是数字签名验证过程,该过程先通过逐级获取 DS 记录,验证域名服务器的公钥,然后进一步利用公钥验证数字签名的正确性。与传统的 DNS 工作过程相比,由于 DNSSEC 增加了数字签名的验证过程,从而可以

辨别 DNS 数据是否真实和完整。

DNSSEC 的主要功能包括: 1) 提供数据来源验证; 2) 提供数据完整性验证; 3) 提供否定存在验证。文献[34]对 DNSSEC 和 NSEC3 安全能力进行了评估, 重点测试 DNSSEC 对缓冲区投毒的抵抗, 并给出了一些建议, 以便最大限度发挥 DNSSEC 的能力。BIND 在目前互联网环境下被广泛使用的开放源码的 DNS 服务器软件, 在处理能力和安全性能方面都不够理想。Nominum 公司研制了一套新型的高性能安全 DNS 系统^[35], 能够在毫秒级延迟的情况下, 每秒处理 100 000 条查询请求, 并且完全兼容 DNSSEC。

DNSSEC 在最初被提出时, 由于技术、成本、网络性能等多方面因素的影响, 一直未得到各方面的充分重视, 部署进展缓慢。随着 DNS 缓存投毒攻击数量及其破坏程度逐年上升, DNSSEC 开始受到广泛重视, 进入大规模部署阶段, 截至 2016 年 12 月 6 日, 互联网根区记录中共有 1 525 个顶级域, 其中 1 376 个完成部署^[36]。

虽然 DNSSEC 在理论上能够很好地解决虚假域名信息的问题, 但由于其部属问题, 导致在应用过程中并没有取得理想的结果, 此外, DNSSEC 没有办法解决 DNS 隐私泄露问题。文献[37]对 DNSSEC 在部署方式上的缺陷进行了评估, 认为 DNSSEC 不适合采取渐进式部署, 难以解决不同域之间的互操作和信息引用问题。例如, 没有部署 DNSSEC 的域将无法解析携带数字签名的资源记录, 而部署了 DNSSEC 的域依然无法判定未携带数字签名的资源记录的真实性。另外, 要求 DNSSEC 在全球范围内, 一次性完成部署也是一个几乎不可能实现的目标, 尤其是在二级域 (TLD)。由于使用了公钥密码体系, 在计算和验证数字签名时, 会引起额外的计算开销和传输开销, 文献[38]进一步测试了 DNSSEC 在计算数字签名时对 DNS 系统功能产生的影响, 发现当大量解析域名时, 频繁地验证计算会增加域名服务器的响应延时, 同时携带大量数字签名的 DNS 应答消息也会占用大量的网络带宽资源。因此, DNSSEC 更容易受到放大攻击的威胁^[39]。

由于 DNSSEC 无法解决传输层面临的威胁, 文献[40]基于 TCP 和 TLS 设计实现了一套 DNS

系统 T-DNS。传统 DNS 系统基于 UDP 传输消息, 由于 UDP 无法限制解析器与服务器之间的会话关系, 在抵御放大攻击、拒绝服务攻击、搭线窃听等方面无能为力。T-DNS 的主要原理是使用 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, 然后在 TCP 会话的基础上使用 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。这种 DNS 的实现方式利用了 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, 同时由于 TLS 的安全传输机制, 解决了内容泄露和恶意篡改问题。T-DNS 尝试借助传输层的安全增强机制来实现 DNS 安全, 不需要修改 DNS 协议, 类似地, 文献[41]以 RFC 草案的方式讨论了基于 TLS 实现 DNS 的相关问题; 文献[42]提出 DNS over DTLS 的实现方案, 利用 DTLS 协议^[43]传输 DNS 的请求和应答消息, 实现信息的保密性。

虽然将加密技术引入 DNS 系统是比较直观的研究思路, 但考虑到系统部署、处理性能等方面, 依然存在许多问题。文献[44]讨论了在 DNS 系统实施加密技术时, 可能存在的误区, 重点对隐私保护、跨域互操作效率和计算/通信开销进行分析。实验结果表明: 1) 现有的许多基于加密技术的 DNS 增强系统没有办法提供隐私保护功能; 2) 由于是渐进式部署, 部分解决方案可能会造成不同域之间在互操作上存在问题; 3) 端到端的加密方案会增加名字服务器的流量开销。

除了基于密码学理论来解决 DNS 信息安全问题, 也出现了一些轻量级的解决方案, 这类方案的特色是不引入密码学方法, 同时也不需要修改 DNS 协议的实现, 易于实现和部署, 但无法提供严格的安全保护。例如, 文献[45]描述了一种新的、实用和简单的技术, 使 DNS 查询更能抵抗投毒攻击, 其工作原理如下: 在查询中混合组成域名字母的大小写, 该方法要求中毒 DNS 缓存的攻击者必须猜测查询的混合大小写编码, 以及 DNS 中毒攻击所需的所有其他字段。这增加了攻击的难度, 被许多 DNS 供应商实施。

2.2.2 系统实现增强

通过修改 DNS 协议来提升系统的安全能力容易受到部署和兼容等问题的困扰, 有学者提出, 在

实际构建 DNS 系统时进行安全增强,这类研究成果的研究思路是通过改善 DNS 生态系统的组成结构和实现方式来提升 DNS 系统的安全防护能力。

文献[46]通过引入认证服务来阻止放大攻击,该方法在域名解析过程中引入认证服务器,所有的域名解析器首先向认证服务器请求挑战字,认证服务器收到请求后,根据域名解析器将要访问的域名服务器为其分配挑战字,并在本地保存相应的挑战字。通过分配挑战字,实现了域名解析器与域名之间对应关系的绑定。在后续的域名解析过程中,认证服务器进一步检查解析请求与挑战字之间的对应关系,并丢弃没有绑定关系的解析请求。通过这种方式,杜绝恶意服务器通过仿冒源 IP 地址进行放大攻击。

文献[47]认为大量存在的开放式 DNS 解析器由于管理不够规范,容易成为攻击者的目标,对整个 DNS 系统造成危害,因此,提出一种解决 DNS 解析器漏洞的方法,即完全删除开放式 DNS 解析器,对用户保留递归查询服务,这样的做法虽然可能导致 DNS 系统整体性能下降,但实验结果表明,为了提升 DNS 系统的安全性,这种牺牲是可以接受的。

文献[48]提出一种顶级匿名 DNS 系统结构 OnionDNS,用于阻止对顶级域名服务器的恶意攻击。与传统的 DNS 系统架构相比,OnionDNS 引入了镜像服务器,镜像服务器位于域名解析器与域名服务器之间,所有的域名解析请求首先被发送到镜像服务器,只有镜像服务器才能获得顶级域名服务器的真实 IP 地址,而域名解析器无法直接访问顶级域名服务器。通过这种匿名的方式,实现对顶级域名服务器的保护。

2.3 诊断监控

对 DNS 系统进行诊断监控不需要改变现有 DNS 协同的实现,具有良好的渐进部署能力,是安全增加解决方案的良好辅助手段。注册恶意域名是许多攻击行为在实施前的第一步,因此,尽早发现恶意域名或者恶意网络域是检测恶意行为的关键技术。

文献[49]设计提出了一套恶意域名检测系统 Kopis,对高层 DNS 服务器之间的流量进行统计分析,通过观察统计指标的变化来识别恶意域名,

其主要原理如下:对于每个 DNS 的域名解析请求 Q_j 以及相应的域名 d 和应答 R_j ,定义一个四元组 $Q_j(d) = \langle T_j, R_j, d, IP_s \rangle$, T_j 用于指定时间单元, $Kopis$ 以一天为一个时间单元, R_j 是发出 Q_j 的主机 IP, d 是要求被解析的域名, IP_s 是应答信息中包含的 IP 地址集合。对于任何一个指定域名 d ,在指定的一段时间内,可以统计出一组数据 $Q_j(d)$, $j = 1, \dots, m$ 。根据这组统计数据, $Kopis$ 计算 3 组统计参数:请求者多样性参数 (RD),表示解析域名 d 的主机的分布情况;请求者权重 (RP),表示与请求者相对应的解析服务器的规模;目标 IP 信誉 (IPR),表示被解析出来的 IP 的信誉值。以请求者多样性参数为例,主要是根据给定的域名 d 和 $Q_j(d)$,先将请求者的 IP 映射到其所属的 BGP 前缀、自治域编号 (AS number) 和国家编号 (CC),然后计算其频率分布情况,进一步计算均值、标准偏差和方差等。如图 1 所示,解析恶意域名与解析良性域名请求者所在自治域的变化情况具有明显的差异。

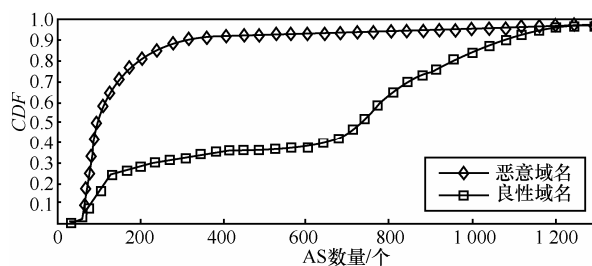


图1 AS多样性频率分布

文献[50]对全球 600 多个分布式递归解析器、超过 260 亿个 DNS 查询/响应消息进行了分析,发现在发给根服务器的查询请求中,有 50% 的请求包含了对畸形 TLD 域名的解析,基于该事实,提出了一套以已知恶意域名为起点,根据 DNS 查询之间的相关性来搜索其他未知恶意域名的方法。文献[51]通过分析域名解析记录的变化以及域名相关的 DNS 查询模式,提出了一些典型的 DNS 解析行为特征,并以此为依据实现恶意域名的早期检测。“Domain Fluxing”是一种通过不停改变和分配多个域名到一个或多个 IP 地址的恶意行为,被许多僵尸网络(如 Conficker、Kraken、Torpig)用于进行资源获取、控制服务器定位等,同时提高自身生存能力。文献[52]针对“Domain

Fluxing”用于自动产生域名的算法进行分析,提出一种方法用于自动检测由算法产生的恶意域名。文献[53]设计一套大规模 DNS 流量被动监测系统 FluxBuster,用于对恶意网络进行早期发现。通过监控分布在不同地理位置的数百个不同网络中的递归 DNS (RDNS) 服务器生成的 DNS 对流量跟踪。

恶意解析行为检测是 DNS 诊断监控研究的另外一项重要研究内容。文献[54]尝试通过测量一些量化指标来分析用户的行为模型,首先对用户群体进行分类,然后通过收集 DNS resolvers 的日志,进行 DNS 的解析请求分析。针对不同群体的用户分析其访问域名的分布特征、访问域名的数量和响应时间的变化情况、不同用户查询请求的交集来分析不同类型用户的 DNS 查询行为之间的关联性。当用户终端产生的 DNS 解析请求没有被直接发送到经过授权的 DNS 服务器,而是被中间人劫持了,用户终端可能会受到虚假的解析应答,文献[55]提出一种检测技术,通过测量应答消息的返回时延来判断当前应答是否来自授权服务器。文献[56]利用 DNS 解析失败来鉴别恶意软件行为,如利用 DNS 通道控制僵尸网络。文章通过分析典型恶意行为,利用 DNS 的工作机理,发掘了一些奇怪的 DNS 解析失败特征,这些特征可以用于判定是否是恶意软件行为。文献[57]提出了一套监测系统,名为 EXPOSURE,对 DNS 进行大规模的流量监测,总结出 15 个重要的流量特征,并以此为依据对域名的使用方式进行分类,判定其是否被恶意使用。为了抑制恶意行为,文献[58]提出一种用于 DNS 的动态信誉系统 Notos,Notos 针对正常使用域名和恶意使用域名的行为建立计算模型,并使用该计算模型结合 DNS 数据流进行信誉计算,通过信誉评价来约束恶意使用域名的恶行为。与基于密码学的方法相比,建立信誉系统不会在域名解析过程中引起复杂的计算开销,是一种轻量级的解决方案,但是,信誉系统具有滞后效应,难以提早发现恶意行为。

2.4 隐私保护

随着越来越多的用户切换到第三方 DNS 解析器(如 Google 公共 DNS 和 OpenDNS),用户

经常访问的站点、感兴趣的信息也可能在域名的解析过程中被泄露。DNS 阻止(DNS blocking)是一种阻止用户定位域名或站点的技术,最早于 1997 年被提出,用于阻止来自未知 IP 地址的垃圾邮件。随着 DNS 隐私保护需求的出现,DNS blocking 技术开始用于这一方面。

文献[59]对 DNS 解析的全过程进行了分析,对每个步骤可能存在的隐私泄露问题进行了归纳,并针对这些问题提出了一种简单灵活的防隐私泄露查询方案 Range Query,该方案采取随机算法将具体的查询内容隐藏在一定的范围中,能够最大程度地降低隐私泄露的可能。文献[60]利用随机噪声和隐私保护查询(PIR)技术来解决 DNS 的隐私保护问题,文献[61]进一步对这 2 种解决方案进行了评估,评估结果表明,第一种方法的优点是简单易实现,缺点是增加了延迟和带宽。而第二种方法需要对 DNS 协议的标准实现进行修改,不具备兼容性。文献[62]提出 EncDNS,一种新颖的轻量级隐私保护名称解析服务作为替代传统的第三方解析器。EncDNS 协议基于 DNSCurve,将加密的消息封装在符合标准的 DNS 消息中。通过利用常规 DNS 解析器向 EncDNS 服务器提供发送者匿名的事实来保护用户隐私。与诸如混合或洋葱路由的传统隐私保护技术不同,传统隐私保护技术由于多跳路由消息而引入相当大的延迟,所以 EncDNS 架构仅引入一个附加服务器实现对现实对手足够级别的保护。文献[63]提出了一个隐私保护 DNS (PPDNS, privacy-preserving DNS),在域名解析过程中提供隐私保护。PPDNS 采用分布式散列表来取代传统的层次结构,使用可计算隐私查询方法(cPIR, computation PIR)。隐私查询方法是指通过诸如同态变化的加密方式实现查询信息对信息提供方保密的一种方法。

目前,解决 DNS 隐私保护的研究成果大多需要对现有 DNS 协议进行改造和扩充,不具备渐进部署的能力。

3 技术挑战

针对 DNS 系统存在的安全问题,虽然已经涌现了大量的研究成果,但不断发生的安全事件和

新出现的攻击行为表明 DNS 安全依然是一个亟待研究和解决的领域, 基于对第2节的总结和分析, 笔者认为 DNS 安全的研究目前在行为分析、渐进部署和开放系统等方面依然存在较多的技术挑战。

3.1 行为分析

DNS 系统在安全防护过程中, 如何识别恶意行为依然是一个难点问题。现有关于 DNS 行为分析成果的研究大多通过流量监测的方式, 结合历史经验来判别已知的攻击行为, 对于恶意行为对 DNS 系统可能造成的危害缺乏量化分析的技术手段。导致这一技术难题的原因包括3个方面。

1) DNS 系统是互联网的基础设施, 为多种应用提供支撑服务, 用户在解析域名过程中产生的 DNS 数据流具有多样性、动态性和二义性等特点, 因此, 难以形成一组固定的具有普适性的评价标准。

2) 用户发出的域名解析请求在到达域名服务器之前, 往往会经过很多中间的解析器, 这些解析器往往对用户不可见, 因此解析路径难以跟踪。

3) DNS 协议缺乏对检测应用行为的必要支持, 如 DNS 协议不会记录查询请求在经过每个解析器和域名服务器时进行的处理动作。

3.2 渐进部署

如何设计支持渐进部署的解决方案, 与现有 DNS 系统兼容运行是 DNS 安全研究的一个关键问题。DNS 系统在最初被设计时, 没有过多考虑安全性问题, 经过多年的发展已经形成了一套规模庞大、结构复杂的生态系统。在这种情况下, 任何不符合 DNS 协议规范的解决方案在实际部署时, 都将面临如何与老系统共生共存的问题。例如, DNSSEC 基于公钥密码技术实现了资源记录的完整性和真实性保护, 能够有效防止缓冲区投毒攻击, 是目前最完善的 DNS 安全解决方案。然而, 由于掌握了 DNS 根区管理权和绝大多数根域名服务器都在美国, 如果 DNSSEC 在全球范围部署, 这将导致互联网关键资源控制权的严重不平等。另外, 目前很多针对 DNS 安全增强的解决方案都需要修改 DNS 协议的实现, 且无法和传统的 DNS 系统兼容运行, 这也为研究成果的推广造成了障碍。事实上, 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%^[64]。

3.3 开放系统

如何有效管理和控制开放的 DNS 系统, 使它们正常、安全地运行, 避免成为攻击者的工具是 DNS 系统安全管理面临的技术挑战。在目前的互联网环境中, 存在大量的开放式 DNS 服务提供商, 这些 DNS 服务提供商的存在, 提高了互联网域名解析的响应速度, 但与此同时, 由于这些 DNS 系统的服务器缺乏统一的安全管理规范和准入控制机制, 很容易被恶意攻击者控制, 发起放大攻击、缓冲区投毒攻击、拒绝服务攻击等恶意行为。因此, 如果规划建成整个互联网 DNS 系统的组成, 在提高性能的同时, 保证整体系统的安全性依然是迫切需要研究的问题。

4 结束语

DNS 的安全运行对互联网的长期健康运行具有举足轻重的作用。本文从脆弱分析、安全增强、诊断监控和隐私保护等方面对 DNS 安全的相关研究成果进行了分析和总结, 并且列举了 DNS 安全研究中的一些具有挑战性的问题, 为进一步的深入研究提供参考。

参考文献:

- [1] BARNES R, SCHNEIER B, JENNINGS C, et al. Confidentiality in the face of pervasive surveillance: a threat model and problem statement[S]. IETF RFC 7624, 2015.
- [2] 王焱, 胡铭曾, 李斌, 等. 域名系统安全研究综述[J]. 通信学报, 2007, 28(9): 91-103.
WANG Y, HU M, LI B, et al. Survey on domain name system security[J]. Journal on Communications, 2007, 28(9): 91-103.
- [3] 单既如, 罗万明. 互联网域名系统安全管理的现状及研究进展[J]. 数据通信, 2009, 2009(2): 17-19.
SHAN J, LUO W. The present situation and research progress of internet domain name system security management[J]. Data Communications, 2009, 2009(2): 17-19.
- [4] 柳青. 我国互联网域名系统的安全问题[J]. 现代电信科技, 2010, 2010(4): 9-11.
LIU Q. The security issues of Chinese DNS[J]. Modern Science & Technology of Telecommunications, 2010, 2010(4): 9-11.
- [5] MOCKAPETRIS P. Domain names concepts and facilities[S]. IETF RFC 1034, 1987, 11.
- [6] DNS RFC [EB/OL]. <https://www.isc.org/community/rfc/dns/>.
- [7] DNS Ecosystem[EB/OL]. https://www.nsrc.org/workshops/2016/nsrc-nicsn-aftld-iroc/documents/prezo/DNS_Org.pdf.
- [8] LEVINE J. DNS blacklists and whitelists[S]. IETF RFC 5782, 2010.
- [9] LEIGHTON T. Improving performance on the Internet[J]. Commu-

- nications of the ACM, 2009, 52(2):44-51.
- [10] 2016 Dyn cyberattack[EB/OL]. https://en.wikipedia.org/wiki/2016_Dyn_cyberattack.
 - [11] Turkey DNS[EB/OL]. <https://blog.radware.com/security/2015/12/turkey-dns-servers-under-attack/>.
 - [12] China DNS[EB/OL]. <http://www.scmp.com/news/china/article/1410423/major-internet-outage-hits-millions-china-cyberattacks-suspected>.
 - [13] Chinese CN[EB/OL]. <http://www.computerworld.com/article/2484097/internet/major-ddos-attacks-cn-domain-disrupts-internet-in-china.html>.
 - [14] ATKINS D. Threats analysis of the domain name system (dns)[S]. IETF RFC 3833, 2004.
 - [15] DNS threat analysis[EB/OL]. <https://www.nlnetlabs.nl/downloads/se-consult.pdf>.
 - [16] Towards improving DNS security, stability, and resiliency[EB/OL]. https://www.internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf.
 - [17] SCHOMP K, CALLAHAN T, RABINOVICH M, et al. Assessing DNS vulnerability to record injection[C]//The International Conference on Passive and Active Measurement. 2014:214-223.
 - [18] Black Ops 2008: It's the end of the cache as we know it[EB/OL]. <https://www.blackhat.com/presentations/bh-jp-08/bh-jp-08-Kaminsky/BlackHat-Japan-08-Kaminsky-DNS08-BlackOps.pdf>.
 - [19] DAGON D, PROVOS N, LEE C, et al. Corrupted DNS resolution paths: the rise of a malicious resolution authority[C]//The Network and Distributed System Security Symposium(NDSS 2008). 2008.
 - [20] XU K, BUTLER P, SAHA S, et al. DNS for massive-scale command and control[J]. IEEE TDSC, 2013, 10(3):143-153.
 - [21] MOHAISEN A. Evaluation of privacy for DNS private exchange[S]. IETF Internet Draft, 2015-05.
 - [22] BORTZMEYER S. DNS privacy considerations[S]. IETF RFC7626, 2015.
 - [23] ROSSEBO J, CADZOW S, SIJBEN P, et al. A threat, vulnerability and risk assessment method and tool for europe[C]//The International Conference on Availability, Reliability and Security. 2007:925-933.
 - [24] KONINGS B, BACHMAIER C, SCHAUB F, et al. Device names in the wild: Investigating privacy risks of zero configuration networking[C]//The International Conference on Mobile Data Management. 2013:51-56.
 - [25] KRISHNAN S, MONROSE F. DNS prefetching and its privacy implications: when good things go bad[C]//The 3rd USENIX Conference on Large-scale Exploits and Emergent Threats: Botnets, Spyware, Worms, and More. 2010:10.
 - [26] BANSE C, Herrmann D, FEDERRATH H. Tracking users on the Internet with behavioral patterns: evaluation of its practical feasibility[M]//Information Security and Privacy Research. Berlin Heidelberg: Springer, 2012:235-248.
 - [27] OpenDNS[EB/OL]. <http://www.opendns.com/technology>.
 - [28] Google Public DNS[EB/OL]. <https://developers.google.com/speed/public-dns/docs/performance>.
 - [29] SCHOMP K, CALLAHAN T, RABINOVICH M, et al. On measuring the client-side DNS infrastructure[C]//The Conference on Internet Measurement Conference. 2013:77-90.
 - [30] PANG J, AKELLA A, SHAIKH A, et al. On the Responsiveness of DNS-based Network Control[C]//The 4th ACM Sigcomm Conference on Internet Measurement 2004. 2004:21-26.
 - [31] CALLAHAN T, ALLMAN M, RABINOVICH M. On modern DNS behavior and properties[J]. ACM Sigcomm Computer Communication Review, 2013, 43(3):7-15.
 - [32] SHULMAN H, WAIDNER M. Towards security of Internet naming infrastructure[C]//Computer Security-ESORICS 2015. 2015.
 - [33] ATENIESE G, MANGARD S. A new approach to DNS security (DNSSEC)[C]//The 8th ACM conference on Computer and Communications Security. 2001:86-95.
 - [34] BAU J, MITCHELL J. A security evaluation of DNSSEC with NSEC3[C]//Network and Distributed System Security Symposium(NDSS 2010). 2010.
 - [35] VantioTM AuthServe. Authoritative DNS [EB/OL]. <http://www.nominum.com/product/vantio-authserve/>.
 - [36] ICANN Research[EB/OL]. http://stats.research.icann.org/dns/tld_report/.
 - [37] HERZBERG A, SHULMAN H. DNSSEC: security and availability challenges[C]//Communications and Network Security. 2013: 365-366.
 - [38] LIAN W, RESCORLA E, SHACHAM H, et al. Measuring the practical impact of DNSSEC deployment[C]//USENIX Security 2013. 2013: 573-588.
 - [39] US-CERT[EB/OL]. <https://www.us-cert.gov/ncas/alerts/TA13-088A>.
 - [40] ZHU L, HU Z, HEIDEMANN J, et al. Connection-oriented DNS to improve privacy and security[C]//ACM Conference on Sigcomm. 2015:379-380.
 - [41] HU Z, ZHU L. HEIDEMANN J, et al. DNS over TLS: initiation and performance considerations[S]. IETF Internet Draft, 2015.
 - [42] REDDY T, WING, PATIL P. DNS over DTLS (DNSoD)[S]. IETF Internet Draft, 2015.
 - [43] RESCORLA E. Datagram transport layer security version 1.2[S]. IETF RFC6347, 2012.
 - [44] SHULMAN H. Pretty bad privacy: pitfalls of DNS encryption[C]//The Workshop on Privacy in the Electronic Society. 2014:191-200.
 - [45] DAGON D, ANTONAKAKIS M, VIXIE P, et al. Increased DNS forgery resistance through 0x20-bit encoding[C]//ACM CCS'08. 2008:211-222.
 - [46] HERZBERG A, SHULMAN H. DNS authentication as a service: preventing amplification attacks[C]//ACM ACSAC'14. 2014: 356-365.
 - [47] SCHOMP K, ALLMAN M, RABINOVICH M. DNS resolvers considered harmful[C]//ACM Workshop on HotNets. 2014:1-7.
 - [48] SCAIFE N, CARTER H, TRAYNOR P. OnionDNS: a seizure-resistant top-level domain[C]//Communications and Network Security. 2015:379-387.
 - [49] ANTONAKAKIS M, PERDISCI R, LEE W, et al. Detecting malware domains at the upper DNS hierarchy[C]//The 20th USENIX Conference on Security. 2011:21-27.
 - [50] GAO H, YEGNESWARAN V, CHEN Y, et al. An empirical reexamination of global DNS behavior[J]. ACM Sigcomm Computer Communication Review, 2013, 43(4):267-278.
 - [51] HAO S, FEAMSTER N, PANDRANGI R. Monitoring the initial DNS behavior of malicious domains[C]//ACM Sigcomm Conference on Internet Measurement. 2011:269-278.

- [52] YADAV S, REDDY A, RANJAN S, et al. Detecting algorithmically generated malicious domain names[C]//ACM Sigcomm Conference on Internet Measurement 2010. 2010:48-61.
- [53] PERDISCI R, CORONA I, GIACINTO G. Early detection of malicious flux networks via large-scale passive DNS traffic analysis[J]. IEEE Transactions on Dependable and Secure Computing, 2012, 9(5): 714-726.
- [54] SCHOMP K, RABINOVICH M, ALLMAN M. Towards a model of DNS client behavior[C]//PAM 2016. 2016:263-275.
- [55] JONES B, FEAMSTER N, PAXSON V, et al. Detecting DNS root manipulation[M]//Passive and Active Measurement. Berlin: Springer. 2016.
- [56] LUO P, TORRES R, ZHANG Z, et al. Leveraging client-side DNS failure patterns to identify malicious behaviors[C]// Communications and Network Security. 2015:406-414.
- [57] BILGE L, KIRDA E, KRUEGEL C, et al. EXPOSURE: Finding malicious domains using passive DNS analysis[C]//The Network and Distributed System Security Symposium(NDSS 2011). 2011.
- [58] ANTONAKAKIS M, PERDISCI R, DAGON D, et al. Building a dynamic reputation system for DNS[C]//Usenix Security. 2010: 18-36.
- [59] ZHAO F, HORI Y, SAKURAI K. Analysis of privacy disclosure in DNS query[C]//The International Conference on Multimedia and Ubiquitous Engineering. 2007:952-957.
- [60] ZHAO F, HORI Y, SAKURAI K. Two-servers PIR based DNS query scheme with privacy-preserving[C]//IEEE International Conference on Intelligent Pervasive Computing. 2007: 299-302.
- [61] CASTILLO-PEREZ S, GARCIA-ALFRO J. Evaluation of two privacy preserving protocols for the DNS[C]//The International Conference on Information Technology: New Generations. 2009: 411-416.
- [62] HERRMANN D, FUCHS K, LINDEMANN J, et al. EncDNS: a lightweight privacy-preserving name resolution service[C]// Computer Security-ESORICS 2014. 2014:37-55.
- [63] LU Y, TSUDIK G. Towards plugging privacy leaks in the domain name system[C]//IEEE 10th International Conference on Peer-to-Peer Computing. 2010:1-10.
- [64] DNSSEC deployment report[EB/OL]. <http://rick.eng.br/dnssecstat/>.

作者简介:



胡宁 (1972-), 男, 湖南长沙人, 博士, 国防科技大学研究员, 主要研究方向为网络与系统安全、计算机网络体系结构、网络管理技术。



邓文平 (1981-), 男, 湖南耒阳人, 博士, 国防科技大学助理研究员, 主要研究方向为网络与系统安全、计算机网络体系结构、高性能路由与交换技术。



姚苏 (1986-), 男, 安徽舒城人, 北京交通大学博士生, 主要研究方向为网络与系统安全、网络安全标准应用技术。