

DNSSEC 自动化部署相关问题分析

郭川, 冷峰

(中国互联网络信息中心, 北京 100190)

摘要: 基于国家顶级域名系统安全扩展协议部署实践, 总结了域名系统安全扩展协议发展背景, 分析了域名系统安全扩展协议当前应用现状, 提出并分析了域名系统安全扩展协议部署中的自动化问题, 总结并分析了在生产环境中部署实施域名系统安全扩展协议时所需要的若干问题。

关键词: 域名系统; 域名系统安全; 域名系统安全扩展协议; 自动化部署

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2017.00155

Analysis of problems in the DNSSEC automation deployment

GUO Chuan, LENG Feng

(China Internet Network Information Center, Beijing 100190, China)

Abstract: Based on the practice of domain name system security extensions protocols' deployment in country code top-level domain, the development background of the domain name system security extensions protocols were summarized, the current applications of the domain name system security extensions protocols were analyzed, the automation problems in the domain name system security extensions protocols' deployment were put forward and analyzed, several issues that need to be addressed when deploying the domain name system security extensions protocols in the production environment were summarized and analyzed.

Key words: domain name system, DNS security, DNSSEC protocol, DNSSEC automation

1 引言

1.1 域名系统介绍

域名系统(DNS, domain name system)是一个提供主机名称(域名)和网络地址(IP地址)之间映射关系的分布式数据库系统。基于DNS还可以提供其他类型的映射服务,如电子邮件服务器、服务类型或主机地理位置等。不夸张地说,几乎所有的互联网应用都会依赖于某种类型的DNS映射查询服务。一次典型的域名解析查询过程如图1所示。

域名系统是一个分层授权管理的、松散耦合的分布式数据库系统。域名系统层级结构如

图2所示。

1.2 DNSSEC 发展背景

域名系统作为互联网络的中枢神经系统,其网络关键基础设施的位置决定了它在互联网中所发挥作用的重要性。域名系统协议设计之初并未考虑过多的安全问题,到20世纪90年代,互联网的商业化进程加速,接入网络中的主机数目突增,域名系统中一直存在的安全问题凸显,其所导致的后果也越来越严重。

1990年,贝尔实验室研究人员Bellovin S M发现DNS协议中存在严重的安全问题^[1],此时DNS已在互联网中广泛部署,此漏洞影响范围又非常广泛,因此,关于此漏洞的正式报告直至

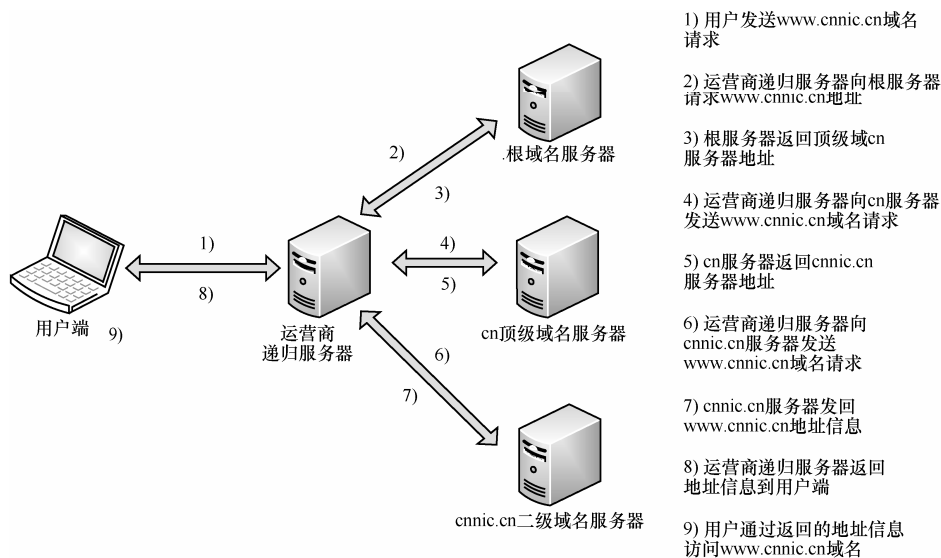


图1 域名查询过程

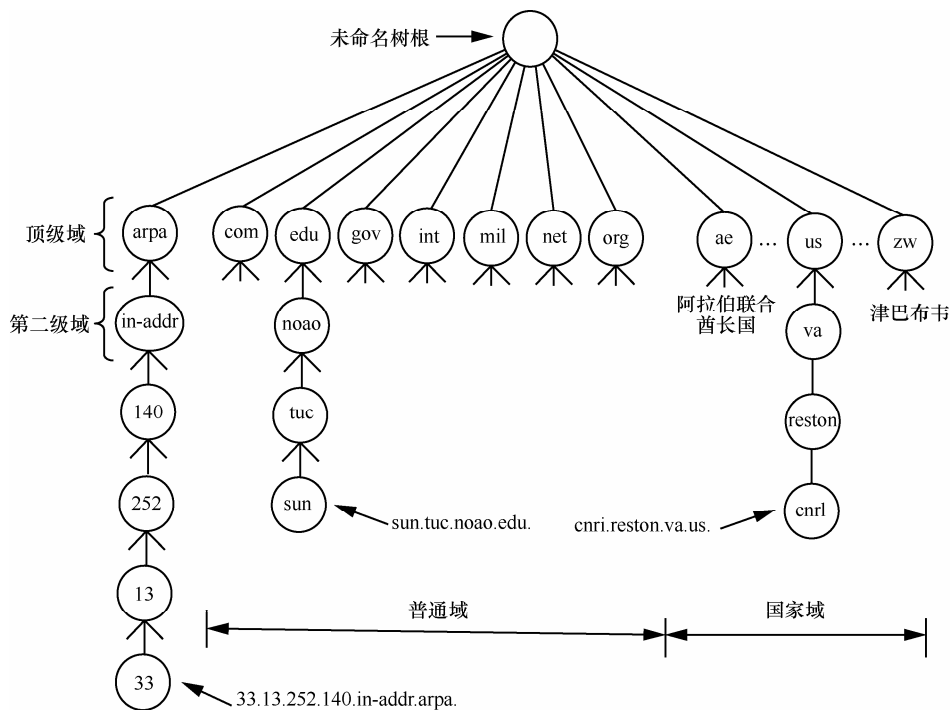


图2 域名系统层级结构

1995年才公开发布^[2]。在此期间，IETF已开始组织域名系统安全扩展（DNSSEC, domain name system security extensions）协议制定活动，Vixie在1995年简单介绍了在此期间IETF相关工作^[3]。1997年，RFC2065的发布，标志着DNSSEC制定活动已基本完成^[4]。1999年，RFC2535的发布，标志着DNSSEC协议已全部完成，BIND9的开发主要用于支持DNSSEC协议^[5]。2000年，瑞典在其国家顶级域中首次尝试部署DNSSEC协议，

但发现存在隐私和扩展方面的问题。随后几年，DNSSEC协议修修补补^[6]，在生产环境中的部署实施进展缓慢。

2008年，安全研究人员发现DNS缓存攻击漏洞，此漏洞利用方法简单有效，影响巨大^[7]。RFC5155随之发布，解决了之前阻碍DNSSEC部署进程的区数据枚举问题^[8]，在相关政府部门和组织机构的大力支持下，各国国家顶级域名及相关域名服务商逐步开始部署实施

DNSSEC 协议。

1.3 DNSSEC 现状及自动化需求

DNSSEC 协议使用了公钥加密的 PKI 体系, 在 DNS 的授权层级中附加了一层认证链, 具体而言, 就是父区对其所有子区的公钥进行签名^[9-12]。DNSSEC 认证链的建立过程如图 3 所示。

全球 13 个根服务器是最早部署实施 DNSSEC 协议的域名服务器, 顶级域名服务器也大多部署实施了 DNSSEC, 目前, 根区数据文件中顶级域名数量为 1 519 个, 其中, 1 370 个已使用 DNSSEC 协议签名, 1 359 个在根区中发布了 DS 记录。顶级域名一般多为各国政府或大型组织所拥有, 具备部署实施 DNSSEC 所需的人力、物力等资源, 但二级域名及以下级域名多为个人或小型组织所持有, 大多不具备部署实施 DNSSEC 所需的技术水平, 此外, 部署实施 DNSSEC 协议大大增加了企业的维护成本, 所以二级及以下层次的域名采用 DNSSEC 协议的现状并不乐观。

DNSSEC 协议设计时并没有考虑增量式部署的情况, 其安全功能是基于所有 DNS 服务器全部采用 DNSSEC 协议这一假设的。如果某个域名从自身向上一直到根区的链条中有某一个区域是没有部署 DNSSEC 协议的, 则 DNSSEC 协议的认证链条无法通达, 从而也就不具备其所提供的安全认证功能。

当前状况是除了根区和顶级域名, 其他二级

域以及以下级域名上采用 DNSSEC 协议认证功能的数量并不乐观。其中一个主要原因就在于部署实施 DNSSEC 协议的复杂性, 如果这一部署过程可以自动化完成, 较少需要人工参与, 会有利于 DNSSEC 协议在全球互联网范围内的部署实施。

2 DNSSEC 自动化问题分析

本节基于国家顶级域名实施 DNSSEC 协议过程中所使用的自动化系统, 指出并分析 DNSSEC 协议自动化部署过程中可能遇到的问题, 以期出现更多的可用于各类场景的 DNSSEC 协议自动化部署实施系统。

2.1 DNSSEC 自动化系统工作流程

DNSSEC 协议最终目的仍旧是提供 DNS 解析服务, 但是在原有 DNS 基础上增加了提供安全验证功能的资源记录, 这些资源记录的生成、存储以及使用, 使 DNSSEC 自动化系统变得更加复杂。DNSSEC 自动化系统工作流程如图 4 所示。

按照图 4 中标识顺序, 介绍 DNSSEC 自动化系统的工作步骤。

- 1) 密钥生成及存储模块自动化生成 DNSSEC 协议所需的 KSK 和 ZSK 密钥对。
- 2) 系统主模块从原始 DNS 资源记录数据存储模块获取区数据信息, 并生成区数据文件。
- 3) 系统主模块将区数据文件发送至密钥生

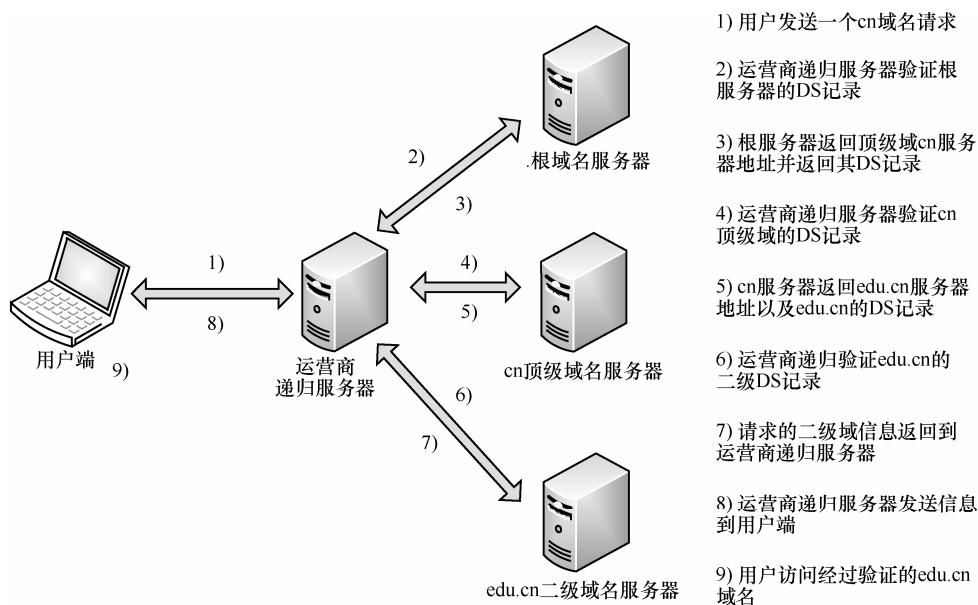


图3 DNSSEC 认证链的建立过程

成及存储模块, 区数据在密钥模块中签名加密, 生成 DNSSEC 区数据文件。

4) 密钥模块将签名完成的 DNSSEC 区数据发送至系统主模块。

5) 系统主模块将 DNSSEC 区数据分发至 DNSSEC 解析服务模块, 对外提供 DNSSEC 解析服务。

6) DNSSEC 解析服务模块向系统主模块发送区数据更新探测请求, 若有更新, 则请求传输更新数据, 否则保持周期性探测请求。

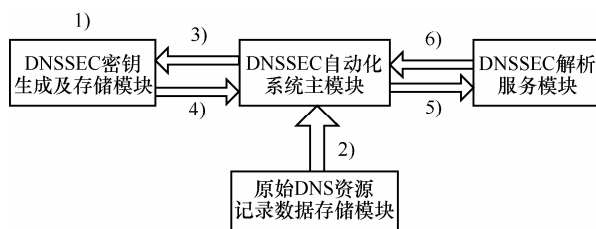


图4 DNSSEC 自动化系统工作流程

此外, 上述工作流程中需要注意的问题有以下几个方面。

1) DNSSEC 协议所用密钥始终存在密钥模块, 不会出现在其他功能模块中, 对其访问也仅限于主系统模块。

2) 原始数据是最终 DNS 服务安全的根基, 原始数据存储模块可能是单独的数据库服务器或存储服务器, 需要注意其安全访问权限。

3) 系统主模块提供可配置的密钥轮转触发功能, 并提供操作接口和监控接口。

4) 解析服务模块可能涉及 anycast 广播的多个服务节点, 具体数据分发方式此处没有具体描述。

2.2 自动化系统主要问题分析

2.2.1 密钥生成及保存

DNSSEC 协议基于公钥加密的 PKI 体系, 公私钥对的生成及保存是部署实施 DNSSEC 时首要考虑的问题。密钥生成需要考虑的主要是其强度, 按照当前业界主流使用情况 (ZSK: 1 024 bit; KSK: 2 048 bit), 结合自身实际, 合理选择即可, 此处不再多述。关于密钥保存, 理想情况下, 私钥应满足离线保存的要求, 但在自动化生产环境中, 区数据签名下发的自动化需求和私钥的离线

保存是相互冲突的。此时, 可以考虑采用专用硬件加密机, 从而既可以满足私钥访问控制, 又可以满足区数据签名自动化需求; 另外一种节约硬件成本的考虑是使用网络访问控制手段, 严格限制存储私钥服务器的访问权限, 如仅限于区数据的输入和签名区数据的输出。

2.2.2 密钥轮转

为了防止密钥泄露, 定期或不定期地更换密钥是有必要的。由于 DNS 系统中缓存服务器的存在, DNSSEC 协议中的密钥更换是个较复杂的问题。密钥轮转的目的是淘汰旧密钥, 使用新密钥, 然而在名称服务器上删除旧的 DNSKEY-RR 以及 KSK 情况下的 DS-RR, 并不能保证密钥在整个 DNS 系统中消失, 它可能仍旧存在于某些缓存服务器中, 使用旧密钥生成的签名记录同样可能仍旧存在缓存服务器中, 这些缓存的记录仅在 TTL 到期或签名失效后才会被删除。因此, 密钥更换主要考虑的问题是权威服务器中密钥、签名数据和缓存服务器中密钥、签名数据需要保持一致性, 从而保证 DNSSEC 认证链的通达。

2.2.3 密钥废除

如果发现当前使用的密钥已泄露, 应启动密钥废除机制。RFC4641 中描述的单一的密钥轮转流程中, 假设旧密钥在轮转期间依然是安全的, 文档中提到的在密钥被破解 (或怀疑被破解) 从而“应急密钥轮转”时, 需要主动的“密钥废除”行动^[13]。在密钥撤销过程中, 旧私钥想必已为攻击者所有并且可被用于伪造区数据; 攻击者重放旧公钥时也不受 TTL 的限制。实际上, 攻击者可以一直重放旧密钥, 直到有关签名记录 (KSK 对应的 DS-RR 的签名, 或 ZSK 对应的 DNSKEY-RRset 记录的签名) 的绝对过期时间到来, 这个时间可能是几天甚至超过一个月。在这之前, 此区及其子区的 DNSSEC 认证都是被污染的。理想情况是尽快废除被破解的密钥。RFC5011 中介绍的多重密钥轮转流程, 同时使用激活和备用密钥^[14]。如果只有激活密钥被破解, 可以废除此密钥并即刻切换到备用密钥。类似地, 如果只有备用密钥被破解, 可以直接废除备用密钥。

2.2.4 NSEC 或 NSEC3

DNSSEC 协议提供否定缓存的认证。最初的

设计是采用 NSEC 方法,但是存在区数据枚举问题,即可以方便地枚举一个区中所有的子域名及对应的资源记录类型,此问题也是 2008 年前很多厂商不愿部署实施 DNSSEC 的一个主要原因。2008 年之后, RFC5155 提出替代方法 NSEC3,基于一定的计算复杂度这一前提,避免了区数据枚举问题^[15]。业界关于区数据枚举是否属于安全漏洞这一问题有不同的看法,有人认为 DNS 数据本就应该公开的,因此也就不存在所谓的区数据枚举问题,但有人认为这会让恶意攻击者获取互联网域名数据及域名注册人信息的困难度大大降低,是个潜在风险。目前看来,针对这一问题并没有达成一致意见,如美国国家顶级域名和巴西国家顶级域名仍旧是使用 NSEC 方式,其他顶级域名大多已采用 NSEC3 方式。NSEC 和 NSEC3 是 DNSSEC 协议中较复杂的问题,可参考 RFC7129 详细地了解^[16]。

2.2.5 资源消耗

DNSSEC 协议会增加服务器的计算、存储资源,也会增加网络带宽消耗。权威服务器在区数据签名过程中需要额外消耗计算资源,解析软件用于存储区数据的内存资源大大增加,区数据的存储及日志存储也需要消耗更多的存储资源。因为签名数据增大了响应数据分组大小,所以也会增加网络带宽消耗。缓存服务器因为需要请求密钥及签名记录并且对签名数据进行认证,所以会增加计算资源的消耗。大型组织多使用 anycast 网络广播方式,此时签名区数据向各广播节点分发也会占用更多网络资源,且分发过程会更依赖于网络质量,因此需要更多的监控服务。

2.2.6 流程可控性

因为 DNSSEC 协议较为复杂,为了更好地管理其各个功能模块,需要对当前及历史执行过程有一个方便的配置和查看工具。在密钥保存服务器上,需要查看密钥当前及历史使用记录,而且可以配置密钥轮转过程中的各类时间参数。对于签名过程,需要针对各个区进行配置,或分别制定资源记录 TTL 参数等。对于签名数据下发,可实时监控各广播节点的数据一致性等。总之,对系统中的各个功能应该模块化,便于定位问题所在;操作又应统一化,便于工作人员具体操作;

监控可视化,便于直观发现问题。

本节结合国家顶级域名部署实践,提出并分析了 DNSSEC 自动化部署实施中需要注意的问题,对密钥生成和保存、密钥轮转、密钥废除、NSEC 或者 NSEC3 的选择、DNSSEC 对占用资源的要求、流程可控等问题进行了简单的介绍和分析,希望能对后续进行此方面工作的相关人员有所参考借鉴作用。

3 未来研究方向

本文主要基于国家顶级域名部署实践分析 DNSSEC 自动化部署相关问题,并没有考虑域名托管服务商同时托管大量域名的场景,此场景下大量域名权威服务器需要分别部署实施 DNSSEC 协议,可能有笔者考虑不到的其他需要注意的问题。

全球互联网名称与地址资源分配机构 ICANN 于 2012 年开启的新一轮新顶级域名申请程序大大增加了根区顶级域名的数量,这一过程中 ICANN 对新申请的顶级域名提出了多种保障其能安全稳定运行的方案,如数据托管、应急恢复等流程,各新顶级域名运行机构技术能力参差不齐,虽然按照 ICANN 要求都有部署实施 DNSSEC 协议,但笔者在本文中并没有针对这一问题做专门分析。

DNSSEC 协议完整认证链的使用除了依赖于各层权威服务器 DNSSEC 协议的部署实施,还依赖于大量各自为政的缓存服务器 DNSSEC 认证功能的开启,缓存服务器在 DNSSEC 认证过程中需要注意的问题,本文未多做介绍。

4 结束语

互联网自 20 世纪 60 年代末期诞生伊始,就存在对名称—地址映射解析的需求,DNS 系统应现实需求而生,严格依赖于域名系统的电子邮件和万维网,自诞生到现在一直是全球互联网中影响最为广泛的应用。DNS 安全问题相较于同属互联网络基础设施层面的 BGP 安全问题,显得更为急迫,因为 DNS 安全问题比起 BGP 安全问题,技术门槛更低也更容易为不法分子所利用,更容易对日常网络用户造成严重不良影响。

DNSSEC 协议集结众多研究人员多年的心血,不仅解决了 DNS 协议本身固有的安全问题,还有望给全球互联网披上一层安全的盔甲,但囿于其复杂性,生产环境部署实施更是进展缓慢。本文基于国家顶级域名 DNSSEC 协议部署实践,指出并分析了 DNSSEC 协议自动化部署实施过程中可能会遇到的问题,希望为后来者参考借鉴。

参考文献:

- [1] BELLOVIN S M. Using the domain name system for system break-ins[C]//Usenix Unix Security Symposium. 1996.
- [2] SCHUBA C L, SPAFFORD E H. Addressing weaknesses in the domain name system protocol[D]. Indiana: Purdue University, 1994.
- [3] VIXIE P. DNS and BIND security issues[C]//Usenix Unix Security Symposium. 1995:263-279.
- [4] EASTLAKE D. RFC 2065: domain name system security extensions[S]. RFC IETF, 1997.
- [5] EASTLAKE D. RFC 2535: domain name system security extensions[S]. RFC IETF, 1999.
- [6] AUSTEIN R. RFC 3833: threat analysis of the domain name system[S]. RFC IETF, 2004.
- [7] US-CERT. Multiple DNS implementations vulnerable to cache poisoning[EB/OL]. <http://www.kb.cert.org/vuls/id/800113>.
- [8] LAURIE B, SISSON G, ARENDS R, et al. RFC5155: DNS security(DNSSEC) hashed authenticated denial of existence[S]. RFC IETF, 2008.
- [9] AUSTEIN R, LARSON M. RFC 4033: DNS security introduction and requirements[S]. RFC IETF, 2005.
- [10] ARENDS R, AUSTEIN R, LARSON M, et al. RFC4034: resource records for the DNS security extensions[S]. RFC IETF, 2005.
- [11] ARENDS R, AUSTEIN R, LARSON M, et al. RFC4035: protocol modifications for the DNS security extensions[S]. RFC IETF, 2005.
- [12] YANG H, OSTERWEIL E, MASSEY D, et al. Deploying cryptography in internet-scale systems: a case study on DNSSEC[J]. IEEE Transactions on Dependable & Secure Computing, 2010, 8(5): 656-669.
- [13] KOLKMAN O, GIEBEN R. RFC4641: DNSSEC operational practices[S]. RFC IETF, 2006.
- [14] STJOHNS M. RFC5011: automated updates of dns security (DNSSEC) trust anchors[S]. RFC IETF, 2007.
- [15] LAURIE B, SISSON G, ARENDS R, et al. RFC5155: DNS security(DNSSEC) hashed authenticated denial of existence[S]. RFC IETF, 2003.
- [16] GIEBEN R, MEKKING W. RFC7129: authenticated denial of existence in the DNS[S]. RFC IETF, 2014.

作者简介:



郭川(1988-),男,河北石家庄人,硕士,中国互联网络信息中心系统工程师,主要研究方向为域名系统安全。



冷峰(1982-),男,山东烟台人,中国互联网络信息中心规划工程师,主要研究方向为域名服务平台优化和域名系统安全。