

在 DNSSEC 下保障顶级域名解析托管服务稳定迁移的操作机制

何峥, 冷峰, 张翠玲

(中国互联网络信息中心, 北京 100190)

摘要: 基于顶级域解析服务托管平台迁移部署实践, 重点研究分析了在 DNSSEC 环境下, 为避免发生域名系统安全扩展 (DNSSEC, DNS security extension) 信任链及解析服务中断、域名 NS 记录不一致等安全问题, 如何在密钥轮转、DS 和 NS 记录变更、数据更新等环节中实现新旧服务托管商及互联网数字分配机构 (IANA, internet assigned numbers authority) 之间进行解析服务平台的迁移, 并对平台迁移操作的关键点进行了详细分析, 提出了在解析托管服务迁移过程中能够保证业务连续性的迁移机制。

关键词: DNS 系统; DNS 安全扩展系统; 密钥轮转; 域名解析; 信任链

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-109x.2021059

Operation mechanism for ensuring the stable migration of top-level domain name resolution hosting services with DNSSEC

HE Zheng, LENG Feng, ZHANG Cuiling

China Internet Network Information Center, Beijing 100190, China

Abstract: Based on the migration and deployment practice of the top-level domain resolution service hosting platform, in order to avoid the occurrence of domain name system security extension (DNSSEC, DNS security extension) trust chain and resolution service interruption, domain name NS record inconsistency and other security issues in the DNSSEC environment, research and analysis was focused on how to migrate the resolution service between the old and new service hosting platform and the internet assigned numbers authority (IANA) without breaking the integrity of the DNSSEC trust chain during the key rollover, DS and NS record changes, data update and other stages. To improve the availability of domain name system services, the key points of the platform migration operation were analyzed in detail, and the migration mechanism that can ensure business continuity during the migration process were proposed.

Keywords: DNS system, DNS security extension system, key rollover, domain name resolution, trust chain

收稿日期: 2020-06-02; 修回日期: 2020-12-18

通信作者: 张翠玲, zhangcuiling@cnnic.cn

基金项目: 北京市科技新星计划项目 (Z191100001119113)

Foundation Item: Beijing Nova Program of Science and Technology (Z191100001119113)

论文引用格式: 何峥, 冷峰, 张翠玲. 在 DNSSEC 下保障顶级域名解析托管服务稳定迁移的操作机制[J]. 网络与信息安全学报, 2021, 7(3): 156-165.

HE Z, LENG F, ZHANG C L. Operation mechanism for ensuring the stable migration of top-level domain name resolution hosting services with DNSSEC[J]. Chinese Journal of Network and Information Security, 2021, 7(3): 156-165.

1 引言

随着域名系统（DNS，domain name system）的发展及应用，许多安全漏洞逐步暴露出来，域名系统成为互联网黑客们有针对性的安全攻击对象，出现了 DNS 缓存污染、DNS 放大攻击及域名欺骗等针对域名服务器的攻击事件。顶级域名服务托管是域名注册管理局将顶级域的五大核心服务托管至具备较强技术能力和拥有稳定平台的域名平台托管机构，确保该顶级域的服务更加稳定安全。当托管平台遭遇物理和网络攻击，造成域名解析平台能力和稳定性无法满足域名注册管理局的要求时，注册管理机构将被动更换域名托管机构，因此变更域名托管机构是不可避免的。随着 2010 年 DNSSEC（DNS security extension）^[1]逐步在全球 13 个根服务器和顶级域名服务器上部署实施，2012 年互联网名称与数字地址分配机构（ICANN，Internet Corporation for Assigned Names and Numbers）开放申请的新通用顶级域也把支持 DNSSEC 协议作为准入门槛，这样极大地增加了域名管理机构迁移域名托管平台的复杂程度，因此在 DNSSEC 环境下迁移域名解析服务成为一个非常棘手的问题。目前，国内乃至国际上的域名服务机构都在积极开展相关技术研究，探索迁移解决方案，而在 DNSSEC 环境下迁移域名解析服务的成功案例并不多见。本文结合顶级域迁移的需求，将顶级域解析服务更换注册局后台托管机构（BERO，Backend Registry Operator）

过程定义了 5 个阶段，重点分析了在 5 个阶段中可能出现的 3 个关键性问题，提出了有效的解决方案，并结合实践经验，提出了一种在 DNSSEC 下保障顶级域名解析托管服务稳定迁移的操作机制。

2 背景

2.1 域名系统及域名托管机构介绍

域名系统是互联网运行的关键基础设施和“中枢神经系统”。DNS 通过域名与 IP 地址之间的对应关系（域名解析，简称解析），为人们提供基于互联网的通信服务。域名系统采用倒置的树形结构自顶向下构建名称，通过分级授权、各域自治的方式进行管理。根位于 DNS 分层结构的顶部，是 DNS 的解析服务的起点与 DNSSEC 信任链的信任锚点；其下依次是顶级域（如“.CN”“.COM”等）及其二级域、三级域等。互联网用户一般通过为其提供 DNS 查询的递归解析服务商获得所需的访问信息。

注册局后台托管机构指为某个顶级域（TLD，top level domain）注册管理局持续提供关键域名注册管理功能的运维机构，保障该顶级域正常解析，确保终端用户的正常访问，与 TLD 注册管理局是不同的组织。2012 年，在 ICANN 推出新通用顶级域（NGTLD，new gTLD）业务（如图 1 所示）后，要求域名平台托管机构具备以下 5 个职能：① 提供托管顶级域的 DNS 解析服务；② 提供托管顶级域的 DNSSEC 应用服务；③ 提供托管顶级域的注册系统；④ 提供托管顶级域的 WHOIS 查

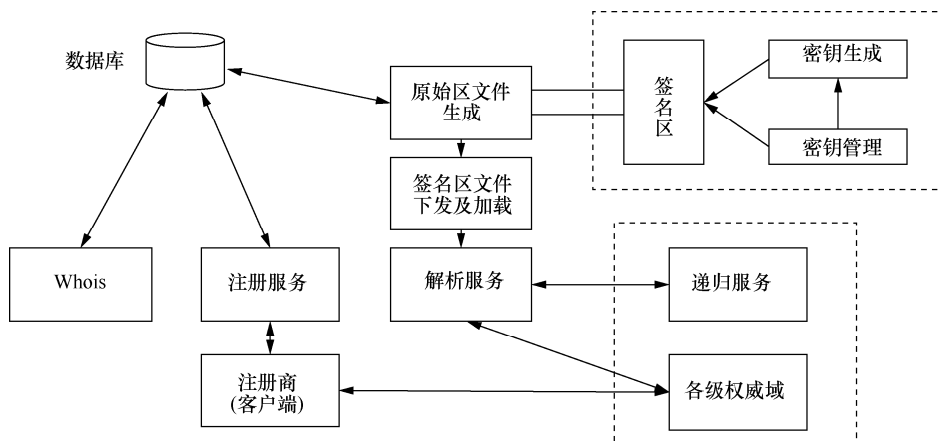


图 1 顶级域部署逻辑示意

Figure 1 TLD registry service framework

询服务；⑤ 协调注册管理机构数据托管服务。

很多企业或组织虽然申请了自己的NGTLD，但并不具备持续提供顶级域五大业务职能的能力。这种情况下，注册管理局可以将自己申请的NGTLD 托管至具备提供上述五大职能的域名托管机构的平台上运维，甚至可以托管至其他国家的域名托管机构。

正如互联网早期的许多协议一样，DNS 协议在设计时缺乏对安全问题的考虑。所以，随着DNS不断发展和应用的增长，暴露了许多安全漏洞，逐渐成为互联网黑客们有针对性的安全攻击对象，出现了DNS缓存污染、DNS放大攻击和洪泛攻击、DNS动态更新攻击及域名欺骗等攻击方式。例如，2008年7月，美国IOActive网络安全公司的计算机安全研究专家Kaminsky公布了DNS系统的一个非常严重的漏洞，该漏洞会导致攻击者轻松地伪造如Google、Gmail等网站，黑客利用该DNS漏洞可能在10s内发起一个“DNS Cache Posion”（DNS缓存中毒）攻击，利用被攻击的DNS服务器能够将用户引导到恶意网站，这就是著名的“Kaminsky事件”^[2]。由于DNS系统极易遭受攻击，这样会造成域名管理机构变更域名托管机构的情况。

2.2 DNSSEC的发展背景

域名系统安全扩展为DNS提供了一种来源

鉴定和数据完整性的扩展，支持对数据源及事务和请求的认证功能，从而在一定程度上遏制了针对域名系统的网络攻击。1995年，国际互联网工程任务组（IETF, The Internet Engineering Task Force）开始组织DNSSEC协议制定活动，由Vixie牵头完成了RFC2065^[3]和RFC2535^[4]的发布，通过使用对称密钥实现了事务级的数据签名，标志着DNSSEC协议已全部完成，BIND9的开发主要用于支持DNSSEC协议。2005年发布的RFC4033-4035^[5-7]提出了DNSSEC，定义了DNSSEC协议使用公钥加密的PKI体系，在DNS的授权层级中附加了一层认证链，利用DNS授权形成的“父子”关系，构建了信任链，实现了基于非对称密钥的DNS数据签名。

DNSSEC在原有DNS系统的基础上，引入了4种主要的记录类型：DNSKEY、DS、RRSIG、NSEC/NSEC3^[8]。其中前3种记录类型为了模仿PKI系统在DNS中加入信任链。最后一种记录为了满足DNS服务的特殊需求，验证“数据不存在”应答的有效性。

由图2可见，DS记录由父区发布，DNSKEY和RRSIG签名记录由子区发布。父区和子区之间通过DS记录和DNSKEY记录产生关联，构成信任链的一环。这个信任链条的初始是信任锚，即认为信任锚是可信的，无须其他验证。在DNS

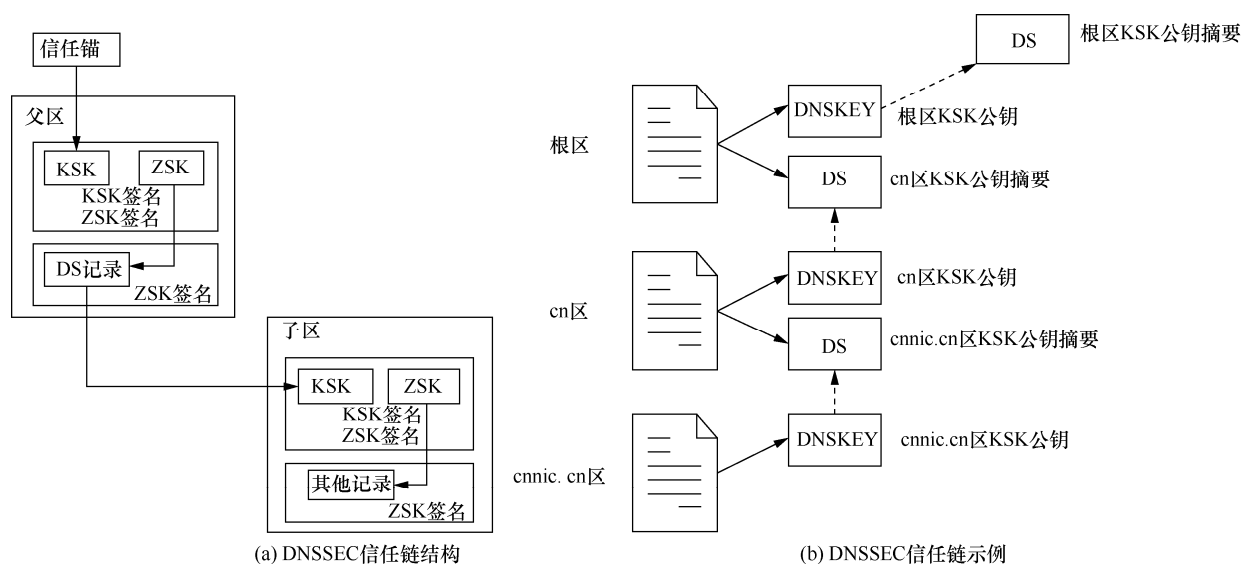


图2 DNSSEC信任链示意图
Figure 2 DNSSEC trust chain

中,这个信任锚可以是任一DS记录或DNSKEY记录,通常设置为根区的DS记录或DNSKEY记录。

由于DNSSEC的部署涉及软件实现的变更,以及服务部署的复杂性,在其被提出的最初几年并没有引起研究人员广泛的兴趣和重视。然而,随着2008年卡明斯基漏洞的公布,DNSSEC的部署显得迫在眉睫,极大地推动了DNSSEC相关协议的软件实现及服务部署。全球13个根服务器是最早部署实施DNSSEC协议的域名服务器^[9],顶级域名服务器也大多部署实施了DNSSEC,2012年ICANN开放申请的新通用顶级域把支持DNSSEC协议作为准入门槛。截至2020年1月,根区数据文件中顶级域名数量为1 514个,其中,1 385个已使用DNSSEC协议签名,1 375个在根区中发布了DS记录^[10],其中1 235个是新gTLD^[11]。国内学者、国家域名注册管理机构以及运营商对DNSSEC的部署和实施进行了研究^[12-14]。

随着云计算、大数据、人工智能、物联网和5G等新技术出现,各种互联网应用层出不穷,对于域名系统这一互联网基础设施的服务稳定性要求越来越高,因此如何避免由于在DNSSEC环境下变更域名托管平台而造成顶级域名解析服务中断的可能,将变成十分棘手的问题。下一节将详细分析域名解析服务的变更过程中可能遇到的问题。

3 顶级域名变更BERO的问题分析

本节基于新通用顶级域在DNSSEC背景下进行解析服务更换BERO的过程,指出并分析解析服务更换BERO过程中可能遇到的问题。

3.1 顶级域解析服务变更BERO的过程

本文主要讨论基于DNSSEC背景下的新通用顶级域解析服务更换BERO的过程。迁移过程涉及TLD迁出方、TLD迁入方及ICANN的IANA机构这3个角色,为了确保整个迁移过程中对数据一致性、DNSSEC信任链完整性、服务连续性的要求,3个角色的操作耦合比较紧密,需要相互配合完成。本文将新通用顶级域解析服务更换BERO的过程定义了5个阶段(状态)。

(1) 新DNSKEY记录发布前(状态1)

(2) 根区发布新DS记录后(状态2)

发布新DS记录之前,根区只有原BERO的DS记录;发布新DS记录后,根区中有新旧BERO的DS记录,标志着新DNSKEY将参与到信任链的验证中。这个阶段为新签名数据的生效做好准备。

(3) 新BERO删除原NS记录后(状态3)

删除原NS记录之前,新BERO的权威服务器上有两组NS记录;删除原NS记录后,新BERO的权威服务器上有1组NS记录。这个阶段是在为原BERO的权威服务器退出解析系统做准备,访问至新BERO的客户端将不再获取到原NS记录。

(4) 根区删除原NS记录后(状态4)

删除原NS记录之前,互联网用户会看到两组NS记录,新旧BERO的权威服务器都将收到查询;删除原NS记录开始,等待TTL时长之后,互联网用户将看不到原NS记录,标志着原BERO的NS服务器正式退出解析系统。

(5) 根区删除原DS记录后(状态5)

删除原DS记录之前,根区中有两条DS记录;删除原DS记录之后,根区中只保留新BERO的DS记录。这是迁移操作的一个收尾步骤,将已不再使用的原DS记录从解析系统中彻底删除。

3.2 变更BERO遇到的主要问题

3.2.1 迁移期间DNSSCE信任链完整性问题

在基于DNSSEC环境下的域名顶级域平台托管机构迁移,增加了确保DNSSEC信任链完整性的要求。顶级域注册管理局在变更域名平台托管机构时,新旧域名顶级域平台将持有各自的私钥,且不会共享彼此的私钥。私钥用于对域名区文件中的权威数据进行签名,对于顶级域来说,权威数据通常包括SOA、NS、DS记录等。当区文件中的权威数据发生变化时,需要对变化的数据进行签名。域名顶级域平台的更换增加了这类操作的复杂性。一方面,因为持有旧密钥和新密钥的是两个不同的单位,他们之间不能共享彼此的私钥,另一方面,为了保证数据的签名始终可以通过验证,必须有旧平台托管机构的配合及签名时的流程与技术保障,否则DNSSEC信任链将中断,无法保证在DNSSEC背景下顶级域名迁移信任链的完整性。

3.2.2 迁移期间解析服务的连续性问题

解析服务的连续性是衡量域名平台托管机构提供的域名服务是否稳定的关键指标。因此在变更域名平台托管机构的过程中, 每一步操作都要确保解析服务的连续性。变更操作涉及的都是权威服务器, 所以往往会忽略对递归服务器端的影响, 特别是新 NS 记录的生效时间、解析数据的 TTL、递归缓存数据过期等问题, 这些都会直接或间接影响解析服务的连续性和可用性。负责根区解析服务的 IANA 将迁移过程中解析服务的连续性和 DNSSEC 信任链完整性作为关键的技术检查内容, 避免对互联网的稳定运行造成严重影响。

3.2.3 迁移期间 TLD 数据一致性问题

顶级域注册管理机构在变更 BERO 时, 需要迁移域名注册服务、域名目录查询服务、域名解析服务、DNSSEC 服务及数据托管服务 5 部分。由于涉及内容较多, 因此更换 BERO 至少需要一个月。域名管理机构为了减小对其服务造成的影响, 往往采用分步迁移的方式进行, 即先完成注册服务、查询服务和数据托管服务的迁移, 再进行解析服务和 DNSSEC 服务的迁移工作。为缩短解析服务的中断时间, 极有可能在新 BERO 与原 BERO 同时提供服务的情况下, 完成注册服务的迁移。在解析服务未成功迁移至新托管机构前, 开通注册服务会导致顶级域数据更新, 极易造成新旧托管机构的解析数据不一致, 这样会对互联网用户造成严重的影响。因此必须考虑如何解决新 BERO 与原 BERO 解析数据一致性的问题。

4 变更 BERO 的实施机制

4.1 提交新旧 DS 记录并预发布新 DNSKEY

在 DNSSEC 背景下顶级域更换 BERO 的过程中, 向 IANA 提交新旧托管机构私钥所生成的 DS 记录和预发布新 DNSKEY 记录并加入区文件这两步尤为关键, 将直接影响 DNSSEC 信任链的完整性。

首先, 为了保证在顶级域解析服务迁移过程的 DNSSEC 信任链不中断, 必须在新旧托管平台上使用各自的私钥对 SOA、NS、DNSKEY 进行

签名; 然后, 向 IANA 提交新旧 DS 记录且生效后, 再进行更换 NS 和更换密钥等过程。对于更换密钥的操作来说, 类似密钥轮转操作, 要解决的关键问题是, 任何时间点递归缓存的数据都能满足如下两个条件:

- 1) 多组密钥及多组签名中, 至少有一组是对应的;
- 2) 多组密钥及多组摘要中, 至少有一组是对应的。

密钥轮转常见的两种方式是预发布和双签。本文采用的是预发布的密钥轮转方式, 双签方式需要签名方同时掌握新旧两套私钥。因顶级域更换 BERO 时无法共享密钥, 所以不能采用双签的轮转方式, 只能采用预发布方式。预发布方式指先在区文件中添加新的 DNSKEY 记录, 确认递归中缓存的旧数据失效后, 再用新 DNSKEY 对应的私钥对数据进行签名, 并替换区文件中的签名。

接下来将结合图 3 对上述内容进行具体的分析。

处于状态 1 时, 权威服务器发布的数据是一组 DNSKEY、一组 RRSIG 和一组 DS。其中 DNSKEY-A 是可以验证 RRSIG-A 的公钥, DS-A 是 DNSKEY-A 的摘要。DS-A $\rightarrow$ DNSKEY-A $\rightarrow$ RRSIG-A 构成了信任链的一部分, 而且可以用于验证。

处于状态 2 时, 权威服务器发布的数据是两组 DNSKEY、一组 RRSIG 和两组 DS。其中 DNSKEY-A 是可以验证 RRSIG-A 的公钥, DNSKEY-B 是预发布的公钥, 计划将来使用。DS-A 是 DNSKEY-A 的摘要, DS-B 是 DNSKEY-B 的摘要。DS-A $\rightarrow$ DNSKEY-A $\rightarrow$ RRSIG-A 构成了信任链的一部分, 而且可以用于验证。DS-B $\rightarrow$ DNSKEY-B 也构成了信任链的一部分, 但由于没有对应的 RRSIG 记录, 所以这条信任链暂时无法验证通过。

递归服务器可能缓存的数据如表 1 所示。如果某个数据未被缓存或已过期, 在取回新数据后, 可以对应至其中一种情况。针对表 1 中的 4 种情况, 能够验证通过的信任链只有一种可能: DS-A $\rightarrow$ DNSKEY-A $\rightarrow$ RRSIG-A。

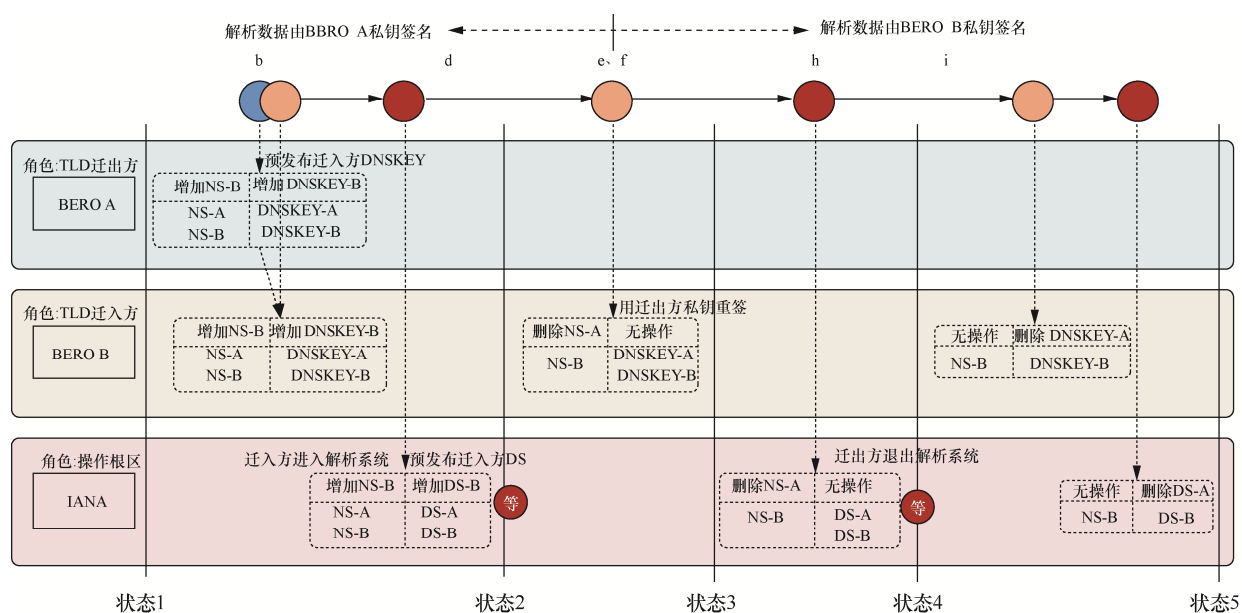


图3 更换 BERO 示意

Figure 3 Procedures of changing BERO

表1 状态1过渡至状态2过程中
递归服务器可能缓存的数据
Table 1 Cache data in recursive DNS
server during state 1 to state 2

可能情况	DS	DNSKEY	RRSIG
1	DS-A	DNSKEY-A	RRSIG-A
2	DS-A	DNSKEY-A	RRSIG-A
3	DS-A	DNSKEY-A	RRSIG-A
4	DS-A	DNSKEY-A	RRSIG-A
	DS-B	DNSKEY-B	RRSIG-B

处于状态3时，由于 BERO A 和 BERO B 的权威服务器同时对外提供服务，数据可能存在一定时间的不同步。BERO A 的 NS 服务器发布的数据是两组 DNSKEY、RRSIG-A 和两组 DS，BERO B 的 NS 服务器发布的数据是两组 DNSKEY、RRSIG-B 和两组 DS。

递归服务器可能缓存的数据如表2所示。如果某个数据未被缓存或已过期，在取回新数据后，可以对应至其中一种情况。针对表2中的情况1，能够验证通过的信任链是 DS-A→DNSKEY-A→RRSIG-A；情况2，能够验证通过的信任链是 DS-B→DNSKEY-B→RRSIG-B。

表2 状态2过渡至状态3过程中
递归服务器可能缓存的数据
Table 2 Cache data in recursive DNS
server during state 2 to state 3

可能情况	DS	DNSKEY	RRSIG
1	DS-A	DNSKEY-A	RRSIG-A
2	DS-B	DNSKEY-B	RRSIG-B

需要注意的是，如果在状态2等待的理论时间需要大于一个 TTL 周期，实际情况考虑网络时延情况应大于 2~3 个 TTL 周期，否则在状态3递归可能缓存的数据如表3所示。如果某个数据未被缓存或已过期，在取回新数据后，可以对应其中一种情况。针对表3中的情况1、情况2，能够验证通过的信任链是 DS-A→DNSKEY-A→RRSIG-A；情况3，能够验证通过的信任链是 DS-B→DNSKEY-B→RRSIG-B；情况4，信任链无法验证通过。可见状态2的等待操作是必要的。

处于状态4时，权威服务器发布的数据是两组 DNSKEY、一组 RRSIG 和两组 DS。其中 DNSKEY-B 是可以验证 RRSIG-B 的公钥，DNSKEY-A 是待清除的公钥。DS-A 是

DNSKEY-A 的摘要, DS-B 是 DNSKEY-B 的摘要。DS-A→DNSKEY-A 构成了信任链的一部分,但由于没有对应的 RRSIG,所以这条信任链无法验证通过。DS-B→DNSKEY-B→RRSIG-B 也构成了信任链的一部分,而且可以用于验证。

表 3 进入状态 3 递归服务器可能缓存的数据
Table 3 Cache data in recursive DNS server during state 3

可能情况	DS	DNSKEY	RRSIG
1	DS-A	DNSKEY-A	RRSIG-A
	DS-B	DNSKEY-B	
2	DS-A	DNSKEY-A	RRSIG-A
		DNSKEY-B	
3	DS-A	DNSKEY-A	RRSIG-B
	DS-B	DNSKEY-B	
4	DS-A	DNSKEY-A DNSKEY-B	RRSIG-B

状态 3 过渡至状态 4 过程中递归服务器可能缓存的数据只有一种情况,如表 4 所示。如果某个数据未被缓存或已过期,在取回新数据后,也是对应这种情况。能够验证通过的信任链是 DS-B→DNSKEY-B→RRSIG-B。

表 4 状态 3 过渡至状态 4 过程中递归服务器可能缓存的数据
Table 4 Cache data in recursive DNS server during state 3 to state 4

可能情况	DS	DNSKEY	RRSIG
1	DS-A	DNSKEY-A	RRSIG-B
	DS-B	DNSKEY-B	

处于状态 5 时,权威服务器发布的数据是一组 DNSKEY、一组 RRSIG 和一组 DS。其中 DNSKEY-B 是可以验证 RRSIG 的公钥,DS-B 是 DNSKEY-B 的摘要。DS-B→DNSKEY-B→RRSIG-B 构成了信任链的一部分,而且可以用于验证。

状态 4 过渡至状态 5 过程中递归服务器可能缓存的数据如表 5 所示。如果某个数据未被缓存或已过期,在取回新数据后,可以对应至其中一种情况。针对表 5 中的 4 种情况,能够验证通过的信任链只有一种可能: DS-B→DNSKEY-B→RRSIG-B。

需要注意的是,如果在状态 4 等待的理论时间需要大于一个 TTL 周期,实际情况考虑网络时延情况应大于 2~3 个 TTL 周期,否则在状态 5 递归可能缓存的数据如表 6 所示。如果某个数据未被缓存或已过期,在取回新数据后,可以对应其中一种情况。针对表 6 中的情况 1、情况 2,能够验证通过的信任链是 DS-A→DNSKEY-A→RRSIG-A;情况 5、情况 6,能够验证通过的信任链是 DS-B→DNSKEY-B→RRSIG-B;情况 3、情况 4,信任链无法验证通过。可见,在没有做数据反向同步的情况下,状态 4 的等待操作是必要的。

通过上述分析可知,在保证等待时间的理论时间大于一个 TTL 周期,实际考虑网络时延情况应大于 2~3 个 TTL 周期的前提下,在迁移的各个阶段,都能保证至少有一条信任链可通过验证,从而保证了 DNSSEC 背景下域名更换 BERO 的信任链完整性。

4.2 提交新旧 NS 记录并写入区文件

由于递归服务器具有缓存功能,其无法实时获知根区和顶级域权威服务器的数据变更。为保证解析服务的连续性,应该在新 BERO 的 NS 记录加入顶级域和根区的解析系统期间,以及在 IANA 删除原 BERO 的 NS 记录之后一段时间,原 BERO 的权威服务器持续在线并正常提供服务。

变更 NS 记录的操作步骤,与 DNSSEC 密钥轮转中的双签操作类似。初始状态为原 BERO 的权威服务器单独提供服务;然后,新 BERO 的权威服务器上线,将 NS 记录添加至顶级域和根区,此时原 BERO 和新 BERO 同时在线提供服务,这个阶段需要等待大于一个 TTL 周期,即顶级域和根区中该 NS 的 TTL 为最大值,才能进入下一阶段;最后,从顶级域和根区中删除原 BERO 的 NS 记录,完成此操作后,在保证等待理论时间大于一个 TTL 周期,实际考虑网络时延情况应大于 2~3 个 TTL 周期,确保两组权威服务器均能正常提供服务。需要注意的是,增加新 BERO 的 NS 记录和删除原 BERO 的 NS 记录时,一定要按照先操作顶级域再操作根区的顺序进行。

表 5 状态 4 过渡至状态 5 过程中递归服务器可能缓存的数据
Table 5 Cache data in recursive DNS server during state 4 to state 5

可能情况	DS	DNSKEY	RRSIG
1	DS-A	DNSKEY-A	RRSIG-B
	DS-B	DNSKEY-B	
2	DS-B	DNSKEY-A	RRSIG-B
		DNSKEY-B	
3	DS-A	DNSKEY-B	RRSIG-B
	DS-B		
4	DS-B	DNSKEY-B	RRSIG-B

表 6 进入状态 3 递归服务器可能缓存的数据
Table 6 Cache data in recursive DNS server during state 3

可能情况	DS	DNSKEY	RRSIG
1	DS-A	DNSKEY-A	RRSIG-A
	DS-B		
2	DS-A	DNSKEY-B	RRSIG-A
	DS-B		
3	DS-A	DNSKEY-B	RRSIG-A
	DS-B		
4	DS-A	DNSKEY-A	RRSIG-B
	DS-B		
5	DS-A	DNSKEY-A	RRSIG-B
	DS-B		
6	DS-A	DNSKEY-B	RRSIG-B
	DS-B		

考虑到 ICANN 要对 EBRO 提交的 NS 记录进行技术检测，因此新旧 NS 记录在根区文件中生效一般需要 5~7 天。只有根区完成新旧 NS 记录加载后，才能进行新旧 EBRO 的迁移，否则可能出现服务中断的情况。

4.3 保证新旧托管平台 DNS 数据文件实时更新

基于实验得出，迁移域名托管平台至少需要持续一个月的时间才能顺利完成。域名管理机构为了减小对其服务造成的影响，往往采用分步迁移的方式进行，即先完成注册服务、查询服务和数据托管服务的迁移，再进行解析服务和 DNSSEC 服务的迁移工作，这样会出现大量变更的解析数据。为了避免发生新旧托管机构的解析数据不一致的情况，建议采用简单有效的 DNS 区传送更新的方式，将在此期间发生的数

据变化同步到新旧托管平台的 DNS 域名服务器。通常的做法是负责产生数据的一方通过 DNS 区传送协议将最新的数据传输给另一方，产生数据的一方指的是维护注册数据库的一方，约定在 IANA 增加 NS 之前是原 BERO，在 IANA 增加 NS 之后是新 BERO，这个问题在有无 DNSSEC 背景的情况下均需考虑。这种状态一直维持到旧 NS 记录从区文件中删除后且递归服务器缓存中旧的 NS 记录已经过期，才能中断 DNS 数据更新。

4.4 DNSSEC 背景下顶级域名解析服务更换 BERO 的实施过程

为了便于实际操作，本文以顶级域“ABC”为例，阐述在部署 DNSSEC 背景下，TLD 更换 BERO（主要涉及 NS 记录、DNSKEY 记录和 DS

记录)的具体操作步骤。

以顶级域 ABC 为例,原 BERO A 有 M 台 NS 服务器,其集合表示为 NS-A, DNSSEC 密钥对应的 DNSKEY 记录为 KSK-A、ZSK-A,其集合表示为 DNSKEY-A, KSK-A 对应的根区中的 DS 记录为 DS-A; 将 BERO A 更换为 BERO B, B 有 N 台 NS 服务器,其集合表示为 NS-B, DNSSEC 密钥对应的 DNSKEY 记录为 KSK-B, ZSK-B,其集合表示为 DNSKEY-B, KSK-B 对应的根区中的 DS 记录为 DS-B。操作步骤如下。

(1) BERO A 和 BERO B: BERO B 的全部 NS 服务器同 BERO A 的全部 NS 服务器建立数据同步关系,数据保持一致。

(2) BERO A: 区数据中增加 BERO B 的 NS 记录、DNSKEY 记录(包括 KSK-A 及 ZSK-A)。

(3) 注册局: 向 IANA 提交申请增加 BERO B 的 NS、DS 记录。

(4) IANA: IANA 将 BERO B 的 NS、DS 记录添加到根区数据中(等待 TTL 时间)。

(5) BERO B: 使用 BERO B 的密钥对区数据签名,并反向同步数据(等待 TTL 时间)。

(6) BERO B: 区数据中删除 BERO A 的 NS、DNSKEY 记录。

(7) 注册局: 向 IANA 提交申请删除 BERO A 的 NS 记录。

(8) IANA: IANA 将 BERO A 的 NS 记录从根区数据中删除(等待 TTL 时间)。

(9) 注册局: 向 IANA 提交申请删除 BERO A 的 DS 记录。

(10) IANA: IANA 将 BERO A 的 DS 记录从根区数据中删除(等待 TTL 时间)。

(11) BERO B: 停止 BERO B 的 NS 服务器和 BERO A 的 NS 服务器的数据同步关系,迁移结束。

注:“等待 TTL 时间”中的 TTL 指根区及 TLD 区中相同记录集 TTL 的最大值。

5 结束语

随着 ICANN 新通用顶级域业务的展开,越来越多的顶级域名实现了 DNSSEC 部署,但近年来大量域名运营机构遭遇网络攻击,造成其不能

正常运转,出现了在实施 DNSSEC 的情况下更换 BERO 的情况。本文指出并分析了顶级域解析平台迁移过程中可能遇到的 DNSSEC 信任链中断、域名解析服务中断、域名 NS 记录不一致等安全问题和迁移过程中与根区数据交互的操作问题,提出了有效的解决方案和迁移操作机制,已成功应用于“成信息”“息在线”“中文网”等十多个顶级域迁移的场景,实现了顶级域迁移过程中的解析服务可用性达到 100%,且确保了顶级域的 DNSSEC 信任链完整性,并在实施过程中通过 ICANN 的全球解析服务监测系统的服务可用性监测。本文为顶级域管理机构迁移解析平台提供了一些经验分享和实践部署步骤。

参考文献:

- [1] 苑朋朋,王常青. DNS 安全威胁及应对措施研究[J]. 网络空间安全, 2018, 9(5): 50-54.
YUAN P P, WANG C Q. Research on DNS security threats and countermeasures, 2018, 9(5): 50-54.
- [2] KOLKMAN O, MEKKING W, GIEBEN R. RFC 6781: DNSSEC operational PRactices[S]. RFC IETF, 2012.
- [3] EASTLAKE D. RFC 2065: domain name system security extensions[S]. RFC IETF, 1997.
- [4] EASTLAKE D. RFC 2535: domain name system security extensions[S]. RFC IETF, 1999.
- [5] AUSTEIN R, LARSON M. RFC 4033: DNS security introduction and requirements[S]. RFC IETF, 2005.
- [6] ARENDS R, AUSTEIN R, LARSON M, et al. RFC4034: resource records for the dns security extensions[S]. RFC IETF, 2005.
- [7] ARENDS R, AUSTEIN R, LARSON M, et al. RFC4035: protocol modifications for the dns security extensions[S]. RFC IETF, 2005.
- [8] LAURIE B, SISSON G, ARENDS R, et al. RFC 5155: DNS security(DNSSEC) hashed authenticated denial of existence[S]. RFC IETF, 2003.
- [9] Root DNSSEC update[EB].
- [10] TLD DNSSEC report[EB].
- [11] New gTLD program statistics[EB].
- [12] 段海新. DNSSEC 原理、配置与部署[J]. 中国教育网络, 2011, (6): 29-31.
DUAN H X. DNSSEC principle, configuration and deployment[J]. China Education Network, 2011, (6): 29-31.
- [13] 段海新. DNSSEC 原理、配置与部署(二)[J]. 中国教育网络, 2011, (7): 34-35.
DUAN H X. DNSSEC principle, configuration and deployment(2)[J]. China Education Network, 2011, (7): 34-35.

- [14] 高二辉, 张跃冬, 何峥. DNSSEC 技术原理及应用研究[J]. 信息安全与技术, 2013, (1): 10-15.

GAO E H, ZHANG Y D, HE Z. The principle and application research of DNSSEC[J]. Information Security and Technology, 2013, (1): 10-15.



冷峰（1982-），男，山东莱阳人，博士，中国互联网络信息中心高级工程师，主要研究方向为域名服务平台优化和域名系统安全。

[作者简介]



何峥（1978-），男，北京人，中国互联网络信息中心高级工程师，主要研究方向为域名系统运行与安全。



张翠玲（1982-），女，山东胶南人，中国互联网络信息中心高级工程师，主要研究方向为域名系统运行与安全。