DNSSec技术发展及应用展望

朱 刚
北京邮电大学 北京 100876

1 DNSSec技术背景

作为互联网基础公共设施之一的域名服务系统，其安全性一直没有得到有效保障。DNS系统自身存在软件漏洞，并且经常遭到如域名劫持、缓存中毒、DDoS（分布式拒绝服务）等攻击，导致整个或部分网络的瘫痪。域名系统受攻击事件层出不穷，近年更是呈愈演愈烈之势。例如，2009年5月8日，易名中国6台DNS服务器遭到黑客攻击，攻击流量超过15 Gbit/s，上万网站无法打开；2009年5月19日，暴风事件造成了江苏、安徽、广西、海南、甘肃、浙江6省网络瘫痪；2009年12月18日，Twitter网站的DNS设置遭到黑客袭击，从太平洋标准时间晚上9:46—11：00，Twitter网站大约80%的访问量都被引向了其他网站。系列安全事件暴露了域名系统作为互联网基础设施的脆弱性。

针对域名系统的安全缺失，全球互联网界寻求DNSSec（Domain Name System Security，域名系统安全协议）来增强域名系统的安全性。IETF在1994年成立DNSSec工作组，并于1999年公布了RFC2535。该协议引入了3种新的资源记录——SIG、KEY和NXT，通过这3个记录的扩展给出一套DNSSec实施方案。2001年，DNSSec工作组引入一种称为授权签名者的认证机制以备取代RFC2535协议，被称为DNSSecbis。2005年发布的RFC4033、RFC4034和RFC4035，分别定义了DNS安全扩展的状况和需求说明、增加的资源记录字段说明以及协议修改说明等。其中，RFC2535的发布是DNSSec的一个里程碑。它第一次建立了一整套以公钥密码体制为基础的DNSSec实施解决方案。目前基于公钥体制的DNSSec设计研究都是以此协议为基础，并逐渐得以发展和完善。

2 DNSSec的全球部署现状

DNSSec自1999年诞生以来，由于技术和机制尚未完善、规模化部署会对网络性能造成负面影响以及设备软件升级和扩容成本高等原因，十余年来一直未得到有效部署。

2008年，Kaminsky漏洞的披露加速了DNSSec的部署进程。Kaminsky漏洞被认为是目前DNS最大的安全性漏洞，利用这种漏洞所发起的缓存中毒攻击这两年也呈爆发之势。针

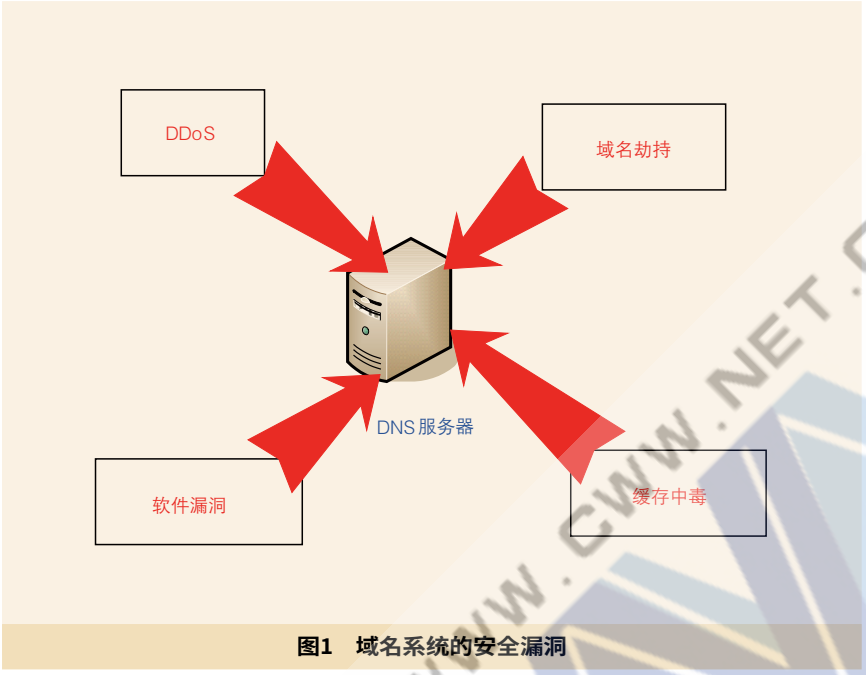

图1　域名系统的安全漏洞

对这种攻击，采用漏洞补丁修复、源端口随机以及增加权威名字服务器的数量等措施，只能是短期行为。解决Kaminsky的长期办法是DNSSec，通过使用数字签名和公共密钥加密机制，提升对应答数据包的弱认证方式以防范缓存中毒。Kaminsky漏洞的揭示所造成的轰动，为互联网界敲响了警钟，极大地推动了DNSSec的发展，是促使DNSSec开始大规模部署的主要催化剂。

目前，DNSSec部署过程已经开启。根服务器（Root）方面，2010年1月，第一台根服务器开始提供已注册的根区域；2010年5月上旬，所有根区域都完成了DNSSec部署，但使用的密钥暂时还不能进行验证；2010年7月15日，ICANN正式发布可用于验证的密钥。

通用顶级域（gTLD）方面，.ORG和.GOV域名已率先使用DNSSec，在互联网使用最为广泛的.COM域名也将于2011年一季度实现对DNSSec的支持。

国家顶级域（ccTLD）方面，美国、瑞典、巴西、波多黎各、保加利亚和捷克等国已完成对DNSSec的部署，并已准备好接收授权签名者记录文件。APNIC从2010年4月14日起启用反向域名根区DNSSec协议。

DNSSec的应用部署是一个渐进的过程，可以预见的是DNSSec与现行的DNS协议仍然会长期共存，因此，在共存期内，未部署DNSSec的区域依然能够使用原有DNS协议进行正常的域名解析。

3　DNSSec不能解决所有DNS安全问题

如图1所示，DNS自身存在软件漏洞，并且经常遭到如缓存中毒、域名劫持、DDoS等攻击。

缓存中毒利用DNS查询记录的缓存机制，在DNS服务器的缓存中存入大量错误的数据记录主动供用户查询。传统的DNS缓存中毒攻击在1990年已出现，但由于攻击所需时间长、成功率低，一直没有引起广泛关注。新型的Kaminsky式攻击克服了这一缺陷，可以对同一域名进行持续攻击，并通过污染目标DNS Cache中权威名字服务器的记录，控制该名字服务器管辖的所有域名主机的查询，破坏力度远高于传统DNS缓存攻击。

域名劫持通常是指通过利用社会工程学或暴力破解，获得某一个域名管理员的账户名称和密码或者域名管理邮箱，然后将该域名的IP地址指向其他的主机。DNS欺骗通常也被归为域名劫持范畴，通过拦截DNS查询请求，发送欺骗性的应答数据包，将受害者要访问的目标机器域名解析为攻击者所控制的机器。

目前针对DNS服务器的拒绝服务攻击主要有两种方式：一种是直接攻击DNS服务器，将DNS服务器作为被攻击对象，由多台攻击主机向被攻击的DNS服务器频繁发送大量的DNS查询请求，最终使DNS服务器崩溃；另一种是利用DNS服务器作为“中间人”去攻击网络中的其他主机，攻击者可以向多个DNS服务器发送大量的查询请求，这些查询请求数据包中的源IP地址为被攻击者IP地址。DNS服务器将大量的查询结果发送给被攻击主机，使被攻击主机无法提供正常的服务，例如使DNS服务器无法为用户提供正常的查询等。

域名服务器软件漏洞经常被攻击者利用，造成DNS服务停止，或者攻击者能够在DNS服务器上执行其设定的任意代码。例如，前段时间针对Linux平台的BIND的攻击程序，就是利用某些版本的BIND漏洞，取得Root权限，一旦入侵完成，入侵者就可以完全控制整个相关的网络系统。

DNSSec并不能解决DNS安全的所有问题。DNSSec可以使用数字签名和公共密钥加密机制有效阻止中间人攻击和域名欺骗，尤其能有效防范2008年披露的Kaminsky式攻击。然而DNSSec对于拒绝服务攻击、软件漏洞以及其他任何类型的利用社会工程学

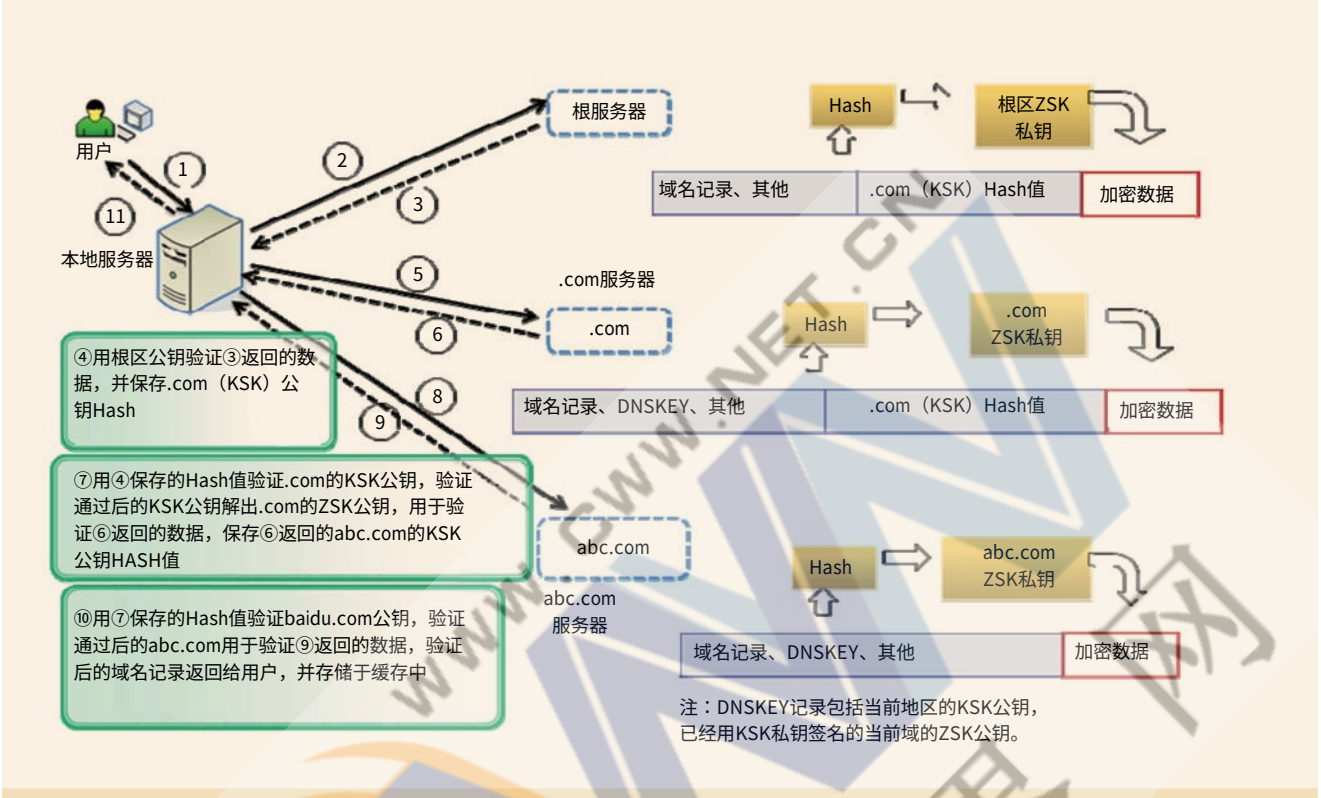

图 2　DNSSec基本工作流程

和基于顶端DNS保护服务的攻击依然无能为力。

4　DNSSec的认证机制

DNSSec在原有DNS上通过PKI技术为每个资源记录集添加数字签名，签名信息与相应的资源记录一起发送给DNS客户端。由于签名信息无法伪造，DNS客户端通过验证应答报文中的签名信息即可判断接收到的信息是否被篡改。

为实现签名与签名验证功能，DNSSec增加了4种新的资源数据类型：RRSIG（Resource Record Signature）、DNSKEY（DNS Public Key）、DS（Delegation Signer）和NSEC（Next Secure）。DNSSec通过增加RRSIG和DNSKEY实现数据完整性保护，客户通过KEY获得某个区的公钥，然后根据KEY来验证某种类型的签名记录，从而保证数据的完整性和数据源的权威性；通过DS存储密钥标签、加密算法和对应的DNSKEY摘要信息；通过NSEC，DNSSec可以针对未知的数据提供可认证的响应，从而使解析器能够对记录不存在的情况进行认证。

DNSSec机制中有两种密钥对，分别为KSK（Key Signing Key，密钥签名密钥）和ZSK（Zone Signing Key，区域签名密钥）。DNSSec使用ZSK来定期计算DNS记录的签名，同时使用KSK来计算ZSK上的签名，以使其可以得到验证。ZSK更新较为频繁（一般一个季度更新一次），以使攻击者难以“猜测”，而期限较长的KSK则经过一个长得多的时段之后才更改（一般2～5年更新一次）。由于KSK对ZSK进行签名而ZSK对DNS记录进行签名，因此只需具有KSK即可对区域中的DNS记录进行验证。它是以DS记录形式传递到“父”区域的一个KSK示例 。父区域（例如根区域）使用自己的、由自己的KSK签名的ZSK对子区域的DS记录进行签名。

DNSSec将一系列数字签名结合到DNS层次化结构中，每一层域名解析过程都需要使用自己的私钥进行加密。DNSSec基本流程如图2所示。

DNSSec基本工作流程如下。

①客户端发起abc.com域名查询请求，如果本地DNS服务器的缓存中存有该条目，则向客户端返回查询结果并结束此次查询。

②如果本地DNS服务器中没有缓存该条目，则向根域名服务器提交查询请求。

③部署了DNSSec的DNS根域名服务器在应答查询请求时，首先使用哈希算法计算应答报文的摘要，再将此摘要用自己的ZSK私钥加密生成签名后

存储到报文中，根域名服务器同时还向DNS服务器返回.com顶级域名服务器的公钥的摘要。

④DNS服务器收到带有签名的应答报文，利用根域名服务器的公钥解密签名获得报文摘要，再将此摘要与从报文数据计算出的摘要进行对比完成数据完整性验证，如果数据完整性验证成功，则同时完成了对数据源（权威DNS服务器）的身份认证，否则身份认证失败。DNS服务器同时把验证通过的.com服务器的公钥摘要存储下来。

⑤⑥的解析与加解密过程同步骤③④。

⑦本地DNS服务器用步骤④保存的Hash值验证.com公钥，验证通过后的.com公钥用于验证⑥返回的数据，同时保存⑥返回的abc.com公钥Hash值。

⑧⑨的解析与加解密过程同步骤③④。

⑩用步骤⑦保存的Hash值验证abc.com公钥，验证通过后的abc.com用于验证⑨返回的数据。验证后的域名记录存储于缓存中。

最后本地DNS服务器向客户端返回查询结果。

DNSSec是由根区域开始的由上至下逐层签名验证，即根区域是整个DNSSec的安全入口，每一个支持DNSSec的客户端解析器都需要建立信任关系。在整个域名查询和相应过程中，每一级DNS服务器都必须对低于它的DNS服务器的密钥进行签名。在验证过程中，DNSSec沿着该信任链一直追溯到根服务器，并自动使用该路径上的“父”密钥验证“子”密钥。

5 部署DNSSec对我国下一代互联网发展的影响

DNSSec是为了解决某些DNS安全问题而出现的，从实际部署、应用情况看，的确起到了很好的作用，尤其是对DNS缓存投毒攻击的遏制方面。我国可以充分利用DNSSec来提升DNS安全防护水平，并进而在政治、经济和互联网研究等领域产生一些积极的影响。

⑴提升我国DNS安全防护水平，推动我国互联网产业发展

据统计，近年来由于DNS缓存中毒攻击等DNS安全问题呈现爆发趋势，严重影响了我国互联网产业的健康发展。通过全面应用、部署DNSSec，能够从根本上对上述DNS安全问题进行遏制，全面提升我国DNS安全防护水平，减少由DNS安全问题所带来的经济损失，推动我国互联网的健康发展。

⑵树立我国互联网大国形象

全面应用、部署DNSSec，构建我国安全可信的互联网环境，将展现出我国作为一个负责任的互联网大国，愿意与国际社会展开合作，共同构建和谐的全球互联网的积极态度，有助于提升我国的国际形象。

⑶推进我国互联网相关的研究

通过部署DNSSec，将会有力地推动我国在域名安全和互联网应急保障等相关技术领域的研究，并最终形成具有自主知识产权的DNS安全防护体系，在未来的互联网发展中赢取更大的话语权。

DNSSec的应用、部署面临着技术方面的困难，具体表现在两个方面。

⑴技术复杂性增加部署难度

DNSSec通过加密数字签名技术实现数据源认证和数据完整性保护，会增加服务器的运算和数据传输开销，原有DNS服务器需要进行性能升级。我国作为互联网大国，境内有以百万计的DNS服务器，如此大规模的性能升级开销巨大。

⑵管理难度增加

DNSSec中使用了公有密钥系统（PKI）来实现协议认证，在应用部署DNSSec后，除原有DNS管理工作外，还必须增加对公有密钥的管理，加大了DNS的管理难度。

6 我国部署DNSSec的建议

在DNS安全问题日益突出、全球DNSSec步入快速部署阶段的背景下，我国也应该顺应国际潮流，积极推动DNSSec部署，并着力推动以下几个环节。

一是积极开展DNSSec试验和应用示范，积累运营管理经验，明确可能存在的问题。DNSSec在部署过程中可能面临众多技术和管理方面的挑战，因此有必要开展相应的应用和示范工程，建立试验环境，识别和解决部署过程中可能带来的技术障碍，测试各种互通和解决方案，确保防火墙、应用和其他设备能够平滑升级。

二是加快完善我国DNSSec标准体系。DNSSec部署涉及到密钥系统的产生、维护和管理过程，公钥分发的具体流程，部署过程中的过渡和互联互通机制，软件和硬件升级等多个方面，在我国大规模部署DNSSec之前，需要先制定完善的标准体系用于指导和规范这些管理和维护流程，以降低DNSSec部署的成本、难度和耗时。

三是加强国际交流和合作。目前国际上根区域和大多数顶级域都已经或即将进行DNSSec的部署，积极参与DNSSec部署的国际交流与合作，一方面有助于借鉴国外部署经验，另一方面也有助于我国尽快加入国际DNSSec安全体系，能够更早地有效防范来自国外的DNS安全攻击。

如对本文内容有任何观点或评论，请发E-mail至editor@ttm.com.cn。