DNS 数据安全解决方案①

许海涛[1,2,3]，金 键[1,2]，毛 伟[1,2]

[1](中国科学院计算机网络信息中心，北京 100190)
[2](中国互联网络信息中心，北京 100190)
[3](中国科学院研究生院 信息学院，北京 100190)

摘 要: DNS 系统当前面临很多安全威胁。介绍了当前主要的两种 DNS 安全解决方案：DNSSEC 和 DNSCurve，对它们进行了全面详细地比较，最后得出结论并提出相应的建议——DNSCurve 在功能上不能代替 DNSSEC，但是可以对 DNSSEC 进行补充，建议在全面部署 DNSSEC 之后，部署 DNSCurve 作为辅助机制。

关键词: 域名系统；DNSSEC；DNSCurve；数据安全；加密算法

Solutions to DNS Data Security Threat

XU Hai-Tao[1,2,3], JIN Jian[1,2], MAO Wei[1,2]

[1] (Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China)
[2] (China Internet Network Information Center, Beijing 100190, China)
[3] (Graduate University of Chinese Academy of Sciences, Beijing 100190, China)

Abstract: DNS system is currently facing many security threats. This paper firstly introduces two major DNS security solutions: DNSSEC and DNSCurve, then conducts a thorough and detailed comparison, finally draws some conclusions which are that DNSCurve cannot substitute DNSSEC but can supplement it, and afterwards makes a proposal which is to deploy DNSCurve as a supplement after the deployment of DNSSEC.

Keywords: DNS; DNSSEC; DNSCurve; data security; cryptographic algorithm

1 引言

DNS(Domain Name System，域名系统)是整个互联网络的基础设施，其主要功能是实现域名地址和 IP 地址之间的转换。DNS 系统的正常运行是 Web 服务、电子邮件服务等众多网络服务正常运行的基础。

作为当前全球最大最复杂的分布式层次数据库系统，由于其开放、庞大、复杂的特性以及设计之初对于安全性的考虑不足，再加上人为攻击和破坏，DNS 系统面临非常严重的安全威胁，因此如何解决 DNS 安全问题并寻求相关解决方案是当今 DNS 亟待解决的问题。

本文首先介绍了 DNS 所面临的安全威胁的主要类型，进而阐述了当前主要的两种 DNS 数据安全解决方案 DNSSEC 和 DNSCurve，并对它们进行了全面详细地比较，最后得出相关结论并提出了相应的建议。

2 DNS安全威胁

针对 DNS 的威胁主要分为以下几类[1]，其中大部分是与 DNS 相关的非常普遍的威胁，有一些则是 DNS 协议特有的。

2.1 DoS 攻击

目前针对 DNS 的 DoS 攻击主要有两种形式：一种是直接攻击 DNS 服务器，将 DNS 服务器作为被攻击对象，由多台攻击主机向所攻击的 DNS 服务器频繁发送大量的 DNS 查询请求，最终使该 DNS 服务器崩溃；另一种是利用 DNS 服务器作为“中间人”去攻击网络中其他主机，又称作放大攻击。攻击者将自身 IP 地址伪装为被攻击者的 IP 地址向多个 DNS 服务器发送大量查询请求，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。

① 基金项目:国家发展改革委员会 CNGI 项目(CNGI-09-03-04)
收稿时间:2010-04-26;收到修改稿时间:2010-05-26

2.2 缓存中毒

DNS 缓存中毒是攻击者利用软件漏洞或者名字服务器配置错误，向 DNS 服务器缓存注入大量错误的数据并能够将错误数据散播到别的服务器，从而引起更多 DNS 服务器中毒的一种攻击形式。由于缓存中的错误数据是由出于不良目的的攻击者所故意伪造的，合法的 DNS 请求方在收到应答后将被指向一个已被攻击者控制的服务器，访问某个特定网站或者带有计算机病毒的文件等。另外，由于 DNS 服务器的 forward 功能（即服务器将针对某域名的查询请求直接转发到指定的服务器进行查询，并利用指定服务器的回应来进行应答），遭受缓存中毒的 DNS 服务器还有可能将错误的记录发送给其他 DNS 服务器，从而导致更多的 DNS 服务器中毒。

2.3 猜测和预测查询(ID Guessing and Query Prediction)

由于 DNS 大都基于 UDP/IP 进行传输，攻击者很容易构造出满足传输协议参数的数据包。DNS 头中的 ID 字段仅有 16 位，而服务器端的 UDP 端口 53 广为人知，所以给定客户端及服务器，ID 号和客户端 UDP 端口号的组合只有 232 种。此外，实际当中 ID 号和客户端 UDP 端口号可以通过之前的数据流进行预测，而且由于防火墙及其他限制，客户端端口号也很可能是一个固定值，这样搜索空间范围减小到了 216，这使得 ID 更容易被攻击者通过强力搜索破获，再结合可能获取的 QNAME 和 QTYPE 信息，攻击者得逞的可能性就大多了。

这种攻击依赖于预测解析器的行为，只有攻击者猜测成功时攻击才能生效，并且攻击者不需要等候在共享网络上。

2.4 不可信的递归服务器

该类攻击是针对下列情形而言的：许多 client 主机只是配置了 stub 解析器，委托递归服务器执行所有的 DNS 查询。在很多情况下递归服务器是由用户的 ISP 提供的。这些递归服务器有可能因为自身存在 bug、已被攻击者控制、出于帮助用户的目的、为了 ISP 及第三方等商业利益等原因向 stub 解析器返回一些用户不期望的响应包，进而造成一定的破坏和困扰。从 DNS 协议的角度来看，这种攻击与数据包拦截等攻击唯一不同点在于这是客户端自愿发送其请求给攻击者的。

2.5 否认存在攻击(Denial of Existence)

该类攻击存在两种情形：1)当 client 请求的名字或记录类型存在时，DNS 服务器应当返回相应的资源记录给 client。而攻击者却伪造响应包告诉 client 它请求的名字不存在，从而屏蔽或阻止了 client 对实际存在的名字的查询；2)当 client 请求的名字或记录类型不存在时，服务器通常返回 nxdomain 或者 nodata 信息给 client，告诉 client 它所请求的数据不存在。而攻击者却伪造响应数据包先一步对 client 请求进行应答使 client 误认为它所请求的数据是存在的并且就是所收到的该应答消息，从而为攻击者下一步更大的破坏做好了铺垫。

3 DNS数据安全解决方案

现有 DNS 数据安全解决方案主要有两种：DNSSEC 与 DNSCurve，下面分别予以介绍。

3.1 DNSSEC

DNSSEC (Domain Name System Security Extensions)[2]，即 DNS 安全扩展协议，是为解决 DNS 安全问题而制定的。它在传统 DNS 协议的基础上引入了四类资源记录(RRSIG, DNSKEY, DS 和 NSEC)和两个消息头标志位(CD 和 AD)，另外为了支持更大的 DNS 数据包提供了对 DNS 扩展机制协议 EDNS0 和 DO 位的支持。DNSSEC 为 DNS 数据提供数据源认证和数据完整性保护，并提供了从 DNS server 到 DNS resolver 的端到端的安全。不过根据设计初衷，DNSSEC 不对 DNS 数据提供机密性保护，仍然以明文传输 DNS 数据包；不提供访问控制机制，不对 DNS client 和 server 进行认证；只保护 DNS 数据的对象安全(object security)，不保护 DNS 事务的隧道安全(channel security)。

3.2 DNSCurve

相比已经是 RFC 的 DNSSEC 而言，DNSCurve 协议[3]目前只是 IETF 的草案 draft。它没有使用传统 DNS 数据包格式而是引入了两种新的数据包格式(Streamlined 和 TXT)，并且不像 DNSSEC 采用 RSA 算法对 DNS 数据签名来提供数据源认证和数据完整性保护，DNSCurve 使用椭圆曲线加密算法 Curve25519 以及随机数 nonce 对 DNS 数据包加密来提供数据的机密性和完整性保护。DNSCurve 提供的是链路级安全，在请求或响应需要经过不可信的 DNS 代理或缓存来

中继的情况下不能提供端到端的安全。总之 DNSCurve 的设计目标是满足 DNS 数据的隐私性需求并通过公钥加密认证机制防止第三方篡改 DNS 数据以保证数据完整性。

4 DNSSEC与DNSCurve的比较

针对目前 DNS 数据安全的两种主要解决方案，下面着重从抗攻击能力、数据机密性、加密算法、数据包格式的向后兼容问题、部署代价及风险、实用情况及应用前景等方面对 DNSSEC 和 DNSCurve 进行比较，具体描述如下。

4.1 抗攻击能力

4.1.1 对 DoS 攻击的抵御

针对第一种 DoS 攻击方式，即针对服务器的 DoS 攻击，DNSSEC 不能抵御，因为它没有访问控制机制，不能设定哪些网段的解析器禁止访问该服务器。同样 DNSCurve 也不能抵御。为了能够对 non-DNSCurve 查询请求进行响应，当 DNSCurve server 验证失败时，会将到来的请求包作为普通的 DNS 数据包进行处理，所以无法抵御此类攻击。针对第二种 DoS 攻击方式，即放大攻击，DNSSEC 同样因为没有访问控制机制不能抵御。而部署了 DNSCurve 的主机则可以抵御。收到响应包时，该主机会使用自身私钥、Server 公钥及随机数 nonce 尝试解密，如果失败则直接丢弃。该过程速度很快，能够抵御此类攻击。

4.1.2 对缓存中毒攻击的抵御

DNSSEC 能够很好地抵御这类攻击。在收到响应包时，解析器首先通过信任链对获取到的 DNSKEY 进行验证，进而验证 DNS 数据签名，从而识别出该数据包是否由权威授权方提供。而 DNSCurve 不能抵御该类攻击。合法的请求方在收到伪造的应答而被指向另一个服务器后将与之进行正常的通讯而不能识别出对方已被攻击者控制，这是因为 DNSCurve 没有 DNSSEC 那样的信任链机制，不能够通过父区来认证对方的公钥。

4.1.3 对 ID 猜测和预测查询攻击的抵御

DNSSEC 能够抵御该类攻击。攻击者基于 ID 猜测及流量分析构造数据包并发往解析器，DNSSEC 解析器收到后对其签名进行验证，经验证失败或者识别出是无效的签名后将丢弃该伪造的响应包。DNSCurve 同样可以抵御该类攻击。攻击者虽然构造了满足传输协议参数的数据包，但是却没有用于加密的由 DNSCurve client 和 server 共享的密钥。Client 收到伪造的数据包后解密失败直接将其丢弃。

4.1.4 对不可信递归服务器攻击的抵御

要抵御该类攻击，stub 解析器或者自己验证 DNSSEC 签名，或者使用隧道安全机制(例如 TSIG)对服务器进行认证来确保它与递归服务器通信的完整性。DNSCurve 不能抵御该类攻击，这是因为它没有信任链机制，不能对递归服务器进行认证。

4.1.5 对否认存在攻击的抵御

对于否认存在攻击的两种情形，DNSSEC 都能够通过验证签名来识别并丢弃伪造的响应包，并且对于第二种情形，将返回 NSEC 或 NSEC3 记录来告诉 client 其所请求的信息确实不存在。DNSCurve 仍然可以通过解密方式丢弃伪造的响应包抵御该类攻击。

综上所述，DNSSEC 和 DNSCurve 对当前 DNS 安全威胁的抵御能力如表 1 所示。

表 1 DNSSEC 和 DNSCurve 的抗攻击能力

攻击 / 对策	DoS 攻击	缓存中毒	ID 猜测及预测查询	不可信递归服务器	否认存在攻击
DNSSEC	不能抵御	能够抵御	能够抵御	有条件抵御	能够抵御
DNSCurve	部分抵御	不能抵御	能够抵御	不能抵御	能够抵御

从表 1 可以看出：DNSSEC 能够抵御缓存中毒攻击并有条件抵御不可信递归服务器攻击(要求 stub 解析器自己验证签名)，而 DNSCurve 则不能抵御这两类攻击；DNSSEC 不能抵御 DoS 攻击反而放大其攻击效果，而 DNSCurve 能够抵御针对网络主机的 DoS 攻击；DNSSEC 和 DNSCurve 均能够抵御其余两种类型的攻击。

4.2 DNS 数据机密性

DNSSEC 不对数据包加密，仍然以明文传输 DNS 数据，不提供任何机密性。DNSCurve 通过加密数据包，使用密文传输 DNS 数据，能够提供一定的机密性

保护。但由于它只是提供链路级安全，只对链路内的DNS 数据进行加密，攻击者依然可以在链路末端(即权威服务器和解析器)获取包括请求方、请求频率、响应方、响应包大小以及所请求的区等信息。这使得DNSCurve 提供的机密性大打折扣。

4.3 加密算法

DNSSEC 采用的加密算法是密钥长度为 1024 位的 RSA。DNSCurve 则使用密钥长度为 256 位的椭圆曲线加密算法 Curve25519。在安全强度上，利用当今最先进的攻击方法，256 位 Curve25519 的攻破难度是1024 位 RSA 的 10 亿倍，其安全强度与 3000 位的 RSA 算法所能达到的安全强度持平；从效率上看，RSA 公私钥长度为 1024 位，加密速度慢，产生的签名较长，消耗 CPU 资源较多；Curve25519 密钥更短，公私钥长度均为 256 位，加密速度很快，产生的签名较短，消耗 CPU 资源更少；从算法成熟度及认可程度来看，RSA 算法是于 1977 年设计的，到目前为止广为使用，安全性经受住了考验；而 Curve25519 是在 2006 年由 Daniel J. Bernstein 在一篇论文中引入的加密算法。目前除 Bernstein 本人之外，对其开展的研究还比较少，其安全性可靠性还有待进一步验证。

4.4 数据包格式的后向兼容问题

DNSSEC 虽然引入了四种新的资源记录及两个标志位，但是没有改变传统 DNS 的消息格式。而 DNSCurve 使用两种全新的数据包格式(Streamlined 和 TXT)，将传统的 DNS 数据包加密后与公钥及随机数 nonce 一起封装，作为扩展了的 DNS 数据包在链路上传输。不过从 client 到 net 之间的设备(例如防火墙)有可能会将不能识别的 DNS 包(例如 DNSCurve 包)直接丢弃。这虽然不是 DNSCurve 自身的问题，但对于其部署或许会带来一些影响。

4.5 部署代价及部署风险

每一种方案的部署都是有代价及风险的。DNSSEC 的部署面临下面代价或问题[4]：

(1) 部署 DNSSEC 意味着一笔巨大的投资。DNSSEC 不能采用渐进式部署，因为只有当一个区之前所有的区都部署了 DNSSEC，才能建立一条从根到该区的信任链，该区才可能从中受益，否则会造成大量的信任孤岛。这要求所有的 zone 管理者同时部署DNSSEC，同时升级服务器及管理软件，DNSSEC 才能发挥其作用。

(2) 投入与收益的不平衡势必会阻碍 DNSSEC 的部署。DNSSEC 部署后并不会带来明显的经济效益，反而会增加区管理者的责任(管理密钥以及生成签名等)，增加 DNS server 的负载，加重 DNS client 的验证负担。真正收益的可能是第三方，因为在他们看来，此时的 DNS 已经是一个能够传输真实数据的相对有效的系统。

(3) DNSSEC 信任模型是分级的也是脆弱的。尽管DNSSEC 允许解析器将除 root 公钥之外的公钥配置为信任锚，但是在一般情况下，root 公钥依然至关重要。对根与某特定名字服务器之间的任何一个区的损害，都会削弱 DNSSEC 对该名字服务器数据完整性的保护能力。

(4) DNSSEC 不能抵御 DoS 攻击反而放大了其攻击效果。DNSSEC 部署后，DNS 响应数据包大小的显著增大、签名及加密等新负担的增加，都使得DNSSEC-aware 服务器更容易遭受 DOS 攻击。

(5) Wildcard RR 在区中的存在极大地复杂化了认证否认机制(Authenticated Denial of Existence)。DNSSEC 虽然使用 NSEC 或 NSEC3 机制提供了对否认存在的验证，但也使得区数据信息更容易泄露给攻击者。

(6) DNSSEC 增加了 DNS 系统的复杂度。潜在的bug 及错误配置的区的数目将进一步增加，使得 DNS 系统面临新的安全风险。

(7) 大规模 TLD 上部署 DNSSEC 面临的问题尤为严峻。ICANN 报告[5]称，在 DNSSEC 部署前后对于1M 规模的 TLD 而言，区规模将膨胀 10 倍左右，服务器加载所需内存将增加 1 倍，BIND 将丢弃 80%的请求，TCP 查询比例将轻微上升。

相比 DNSSEC 巨大的部署代价而言，DNSCurve 部署代价从目前看来要小得多。它只需在解析器上安装 DNSCurve cache 软件，在服务器上或前端安装 DNSCurve forwarder 软件，并进行简单的配置即可。

4.6 实用情况及应用前景

从实用情况和应用前景来看，DNSSEC 协议从 1993 年开始对其研究，目前是 IETF RFC，截止到 2009 年 7 月份，已经在 10 多个国家顶级域及通用顶级域上得到了部署。根据 ICANN 公布的时间表，2010 年 7 月 1 号之前将实现其在根区的全面部署。此外，还得到了 BIND、NSD、Unbound 等众多 DNS 软件的支持。

DNSCurve 提出较晚，实现较少，在业界获得的支持与 DNSSEC 相差很大。截止到 2010 年 2 月，只有 OpenDNS 声称已经实现和部署了 DNSCurve。因此 DNSCurve 很少有机会得到广泛部署，更不用说在根服务器上进行部署了。

5 结论及建议

综上所述，DNSCurve 采用加密方式来增强 DNS 的安全。它有如下优点：1)能够为 DNS 数据提供有限的机密性保护；2)能够抵御针对网络主机的 DoS 攻击；3)与 RSA 算法相比，其采用的加密算法 Curve25519 具有密钥短、安全等级高、加密速度快、生成签名短以及计算资源消耗少的优点；4)公钥分发机制比较独特，或许能够为其他协议的公钥分发机制提供参考；5)部署代价就目前看来比较小。但是也存在着不少缺点：1)提出较晚，除 OpenDNS 外，没有更多的部署；2)所采用的加密算法在安全性、灵活性上没有得到大量验证，更没有被广泛使用；3)不能抵御缓存中毒攻击以及不可信递归服务器攻击；4)数据包格式不能与传统 DNS 向后兼容，在传输时会面对被丢弃的风险；5)开展研究较晚较少，大量的安全风险有待发现和解决。

而 DNSSEC 协议存在也存在不少缺点，如协议复杂、信任模型脆弱、放大 DoS 攻击效果、以及部署代价高等。但是与 DNSCurve 相比具有下列优势：1)提供端到端的数据源认证和完整性保护，能够解决包括缓存中毒攻击在内的大部分现有的 DNS 安全威胁；2)开展研究较早，对其优缺点及部署代价均有很全面细致的研究；3)已经在多个顶级域上得到了部署，并得到 ICANN、BIND 等国际组织和商业软件的大力支持；4)对 DNSSEC 的研究仍在大力开展，目前面临的问题有望得到进一步解决。

鉴于二者各有优缺点，关于如何解决 DNS 数据安全问题有如下建议：1)考虑用加密算法 Curve25519 代替 RSA 成为 DNSSEC 的加密算法。2)在 DNSSEC 全面部署之后，部署 DNSCurve 作为辅助机制，一旦 DNSSEC 信任链因某种原因而断裂时，可以启用 DNSCurve 来暂时保证 DNS 数据安全。3)同时部署 DNSSEC 与其他隧道安全机制，从而更系统全面地增强 DNS 安全性。

6 结语

DNS 系统面临着很多安全威胁。针对那些 DNS 安全威胁，科学界已经提出了许多解决方案，其中 DNSSEC 是最有影响并且最有可能得到广泛部署的解决方案。而 DNSCurve 是最近提出的 IETF 草案，也声称能够解决 DNS 安全威胁问题，目前已引起广泛关注。本文正是基于这种背景对 DNSSEC 和 DNSCurve 两种方案进行了详细地比较和分析，对解决 DNS 安全威胁提出了相应的建议，这对于有效增强 DNS 安全是有意义的。

参考文献

1 Atkins D, Austein R. Threat Analysis of the DNS, RFC 3833, 2004.

2 Arends R, Austein R, et al. DNS Security Introduction and Requirements, RFC 4033, 2003.

3 Dempsky M. DNSCurve: Link-Level Security for the Domain Name System, Internet Draft, 2004.

4 Yang H, Osterweil E, et al. Deploying Cryptography in Internet-Scale Systems: A Case Study on DNSSEC, 2009.

5 Wessels D, Sisson G. Root Zone Augmentation and Impact Analysis, 2009.