综述

DNSSEC 技术发展及影响分析

崔淑田[1],刘　越[2]

(1.中国人民大学经济学院　北京 100872;2.工业和信息化部电信研究院　北京 100191)

摘　要　首先从域名系统(DNS)存在的安全问题入手,对 DNS 安全扩展(DNSSEC)协议技术及其安全性能进行分析,从全球角度介绍了 DNSSEC 的部署进程和发展趋势,分析了 DNSSEC 存在的问题和不足,并针对我国提出了应对 DNSSEC 发展的策略建议。

关键词　域名系统;域名系统安全扩展;安全保护;互联网治理

1　DNS 及其面临的安全问题

1.1　DNS 简介

域名系统(domain name system,DNS)是互联网上最为重要的关键基础设施之一,完成域名到 IP 地址的映射,具有较高的查询和管理效率,方便人们使用各种网络应用[1]。DNS 服务发展迅速,已经成为全球最大也是最为成功的分布式数据库系统。

域名体系采用反向树形结构,其顶层为根域名,在书写域名时默认为省略;根域名之下为顶级域名,顶级域包括国家和地区顶级域(country code top level domain,ccTLD)和通用顶级域(generic top level domain,gTLD);域名注册人可在顶级域下注册二级或二级以下的域名。将一条从叶到根的路径上的各级名称用"."分隔连缀起来,就构成一个独一无二的完整域名,这棵逆向树就称为域名空间,域名则是存放在被称为资源记录(resource record,RR)的数据结构中。

域名空间被分成若干个区(zone),每个区按其管辖范围拥有域名空间相应部分的完整信息。每个区必须指定一个主(primary/master)DNS 域名服务器来负责本区内的域名解析,资源记录就保存在域名服务器的 zone 文件中。辅助 DNS 服务器从具有该区授权的域名服务器(通常是主 DNS 服务器)上获得所在区的数据,并通过定期查询主 DNS 服务器以保证所存储的区数据为最新版本。主服务器和辅助服务器统称为权威 DNS 服务器。

通过分层结构和分级授权机制,DNS 分布地 DNS 采用客户机/服务器机制进行域名解析的查询和应答。域名服务器作为服务器端,为客户端完成 DNS 分布式数据的存储和解析,包含各级权威服务器和缓存服务器。解析器位于客户端,负责执行解析请求,即接受来自客户端应用程序的 DNS 查询请求,向域名服务器发送查询请求,并负责接收域名服务器的返回信息,将结果发给客户端的应用程序。各级域名服务器和解析器构成了 DNS 的基础设施。

1.2　DNS 的安全问题

DNS 协议是至关重要的互联网基础协议,已被广泛使用。但作为 Internet 的早期协议,DNS 被设计为建立在互信

表 1 DNS 事务及其所面临的威胁、安全目标和 IETF 安全规范

DNS 事务	威胁	安全目标	IETF 安全规范
DNS 查询/响应	伪造的或虚假的响应； 移除响应中的资源记录； 通配符扩展规则的不正确应用	数据源授权； 数据完整性验证	DNSSEC
区传送	(分布式)拒绝服务攻击； 消息篡改	双向授权； 数据完整性验证	TSIG
动态更新	非授权更新； 消息篡改； 重放攻击	双向授权； 数据完整性验证； 签名的时间戳	TSIG 或 SIG(0)
DNS 通知	虚假通知	防止由于通过增加工作量导致的拒绝服务攻击	指定可从哪些主机接收信息 TSIG 或 SIG(0)

模型基础之上的开放体系结构，缺乏适当的信息保护和认证机制。由于 DNS 对于互联网的重要性以及自身的脆弱性，针对 DNS 的攻击近年来呈现上升的趋势，其安全性不容乐观。DNS 面临的主要威胁、安全目标和相应的国际互联网工程任务组(IETF)安全规范如表 1 所示[2]。

2 DNSSEC 技术及其安全性能分析

2.1 DNSSEC 概述

DNS 安全扩展(domain name system security extension，DNSSEC)协议是 IETF 开发的，提供了一种通过软件来验证 DNS 数据在互联网传输过程中未被更改的方式。DNSSEC 的研究始于 20 世纪 90 年代，1999 年 IETF 发布 RFC 2535[3]，提出了以公钥密码机制为基础的 DNSSEC 实施解决方案。DNSSEC 协议通过使用公钥基础设施(public key infrastructure，PKI) 在原有的 DNS 基础上添加数字签名(digital signature)，对通过 DNS 体系内部的信息同时提供权限认证和信息完整性验证，能够部分地解决 DNS 存在的安全问题。

DNSSEC 的主要功能有 3 项：

- 提供数据来源验证——DNS 数据来自正确的域名服务器；
- 提供数据完整性验证——数据在传输过程中没有任何更改；
- 提供否定存在验证——对否定应答报文提供验证信息。

基于 DNSSEC 的域名解析过程，服务器端将把签名信息和查询到的 DNS 原始信息一起发送给客户端。由于签名信息无法伪造，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安全。

2.2 DNSSEC 的工作原理

采用 DNSSEC 机制的 DNS 服务器 (一般是区内的主服务器)首先基于公钥加密系统产生一对密钥，其中一个为公钥，另一个为私钥。公钥对外进行公开发布，任何人均可获得并使用；私钥由主服务器的管理员或管理机构负责保管，严格对外保密。

DNS 服务器用私钥对返回给查询方的资源记录(RR)进行数字签名得到一个新的资源记录(RRSIG)，并将经过签名的 RRSIG 与未经签名的 RR 作为应答报文一起发送给提出查询请求的客户端或解析器。RRSIG 中还包含有公钥或数字签名算法的代码。收到应答报文的客户端或解析器可以利用公钥和加密算法对收到的 RR 进行加密运算，可以得到一个计算出来的 RRSIG，将其与所收到报文中的 RRSIG 进行比对，如果二者相同，则通过了对签名者的认证并验证了数据的完整性，即应答报文中的 RR 是真的，否则就说明收到的 RR 是假的。

在 DNSSEC 的实际运行中，每个区需要双重密钥[4]，第一对密钥用来对区内的 DNS 资源记录进行签名，称为区签名密钥(ZSK)；第二对密钥用来对包含密钥(如 ZSK)的资源记录(DNSKEY)进行签名，称为密钥签名密钥(KSK)。在 DNSSEC 中，解析器必须信任所收到的公钥，才能用其进行解密从而验证数据的完整性。解析器首先用 KSK 公钥验证 DNSKEY，然后用 ZSK 公钥来验证数据。因此，KSK 公钥成为 DNSSEC 的关键入口。如果解析器信任它所使用的 KSK 公钥，则这个 KSK 公钥就称为这个解析器的信任锚(trust anchor)。启用 DNSSEC 的区(或称签名区)将自己的 KSK 公钥交给父区，由父区用自己的 ZSK 私钥对其进行签名；同样地，父区也可以将自己的 KSK 私钥交由自己的父区，由其用 ZSK 私钥进行签名。这样的过程称为安全

授权,当这个过程向上到达信任锚的时候,就形成了一条信任链(trust chain)。由于 DNS 所具有的层级结构,根区位于最顶端,且具有唯一性,因此根区的 KSK 公钥就自然而然地成为所有区的信任锚。这样,当一条信任链一直通达根区时,表明这条链上的各级区域都是可以信任的,能够用根区的 KSK 公钥对其进行签名验证从而确保数据来源的可靠性和数据本身的完整性。在理想情况下,如果所有的区都部署了 DNSSEC,则解析器只需保存作为信任锚的根区 KSK 公钥就可以依次进行验证,确保自己确实是从需要的 DNS 服务器那里得到了应答报文。

为了保证和查询相应的资源记录是确实不存在,而不是在传输过程中被删除,DNSSEC 机制提供了一个验证资源记录不存在的方法。它生成一个特殊类型的资源记录:NSEC(nert secure)。NSEC 记录中包含了域区文件中它的所有者相邻的下一个记录以及它的所有者所拥有的资源记录类型。这个特殊的资源记录类型会和它自身的签名一起被发送到查询的发起者。通过验证这个签名,一个启用了 DNSSEC 的域名服务器就可以检测到这个域区中存在哪些域名以及此域名中存在哪些资源记录类型。

为了保护资源记录中的通配符不被错误的扩展,DNSSEC 会对比已验证的通配符记录和 NSEC 记录从而来验证名称服务器在生成应答时的通配符扩展是正确的。

2.3 DNSSEC 的安全性分析

DNSSEC 所使用的 PKI 是基于非对称密码学设计的,其密钥具有这样的性质:用公钥加密的文件只能用私钥解密,而私钥加密的文件只能用公钥解密。公钥和私钥成对产生,相互具有唯一性;而且由于非对称密码的技术特点,加密简单方便,解密则只能通过最为原始的穷举法对密钥(私钥)进行猜测,而不能在已知公钥和加密结果(在 DNSSEC 中是数据经过 ZSK 加密后得到的 RRSIG 和密钥经过 KSK 签名后得到的 DNSKEY)的前提下通过推导得出私钥。

DNSSEC 的安全性取决于 PKI 所用密钥的安全性。由于 PKI 所具有的密码学性质,PKI 的保密性(或称安全强度)取决于密钥(一个二进制序列)的位数,位数越长,意味着破解所花费的时间或者消耗的计算资源越多,因而安全强度越大,保密性越好。

根据有关信息安全标准的建议,DNSSEC 选择了 RSA/SHA-*n* 这一最为常用的 PKI 算法[4],即首先将要传送的数据通过 SHA-*n* 算法进行安全散列变换,然后利用 RSA 算法生成的公钥进行数字签名。随着时间的推移,计算能力不断提高,为了防止被破解,密钥的位数将逐渐加长(如表 2 所示)。

表 2 DNSSEC 所用的 PKI 算法及安全强度

时间	安全强度(bit)	数字签名算法	散列算法
2010 年之前	80	RSA 1024	SHA-1
2010–2030 年	112	RSA 2048	SHA-256
2030 年之后	128	RSA 3072	SHA-256/512

2.4 部署 DNSSEC 的主要影响

DNSSEC 提供了端到端的完整性和真实性签名验证,能够较为有效地防止 DNS 欺骗,大大增强了 DNS 解析过程的安全性,是目前比较完善的 DNS 安全解决方案。从当前国际上的发展情况来看,DNSSEC 作为保障域名体系安全的一项技术正在获得越来越广泛的认可和应用,这有助于增强 DNS 的安全性,减少政府、商业机构和广大用户所受到的网络安全威胁,促进电子政务、电子商务和各类网络应用的发展。

但同时也需要看到,由于 DNSSEC 的信任机制,一旦全球 DNSSEC 部署完毕,根区的信任锚就成为 DNS 安全解析的入口或起点。根据与美国政府签署的有关合同,注册在美国的互联网域名地址分配机构 ICANN 和 VeriSign 公司参与根区 DNSSEC 部署进程并负责根区密钥的管理。这意味着已经掌握了 DNS 根区管理权和绝大多数根域名服务器的美国,借提高 DNS 安全的名义,通过 DNSSEC 进一步增强其对互联网关键资源管理权的控制,将继续保持其优势地位。根区 DNSSEC 部署及管理架构如图 1 所示。

除去政治和安全目标外,部署 DNSSEC 需要利用先进密码技术并进行大量的软硬件升级,将有利于掌握核心技术的国家与企业扩大其在网络和信息安全的影响力,继续占据技术和市场的领先地位。

3 DNSSEC 的部署进程和发展趋势

3.1 DNSSEC 部署工作近年来推进较快

1999 年 RFC 2535 发布后的近 10 年间,DNSSEC 受限于技术、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。2008 年 Kaminsky 漏洞的发布轰动了业界,而利用这一漏洞所发起的 DNS 缓存中毒攻击数量及其造成的损失近年来也在大幅度上升。DNSSEC 作为解决这一漏洞的主要办法因而受到了广泛重视,开始进入大规模部署阶段,且呈现加速之势。

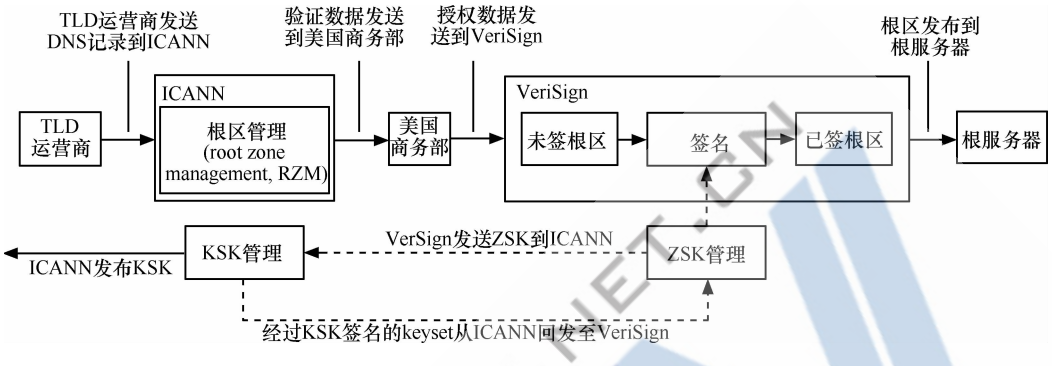

图 1 根区 DNSSEC 部署及管理架构

(1)根区 DNSSEC 部署完成,信任锚正式启用

2010 年 6 月 16 日,ICANN 在位于美国东部弗吉尼亚州卡尔佩帕(Culpeper)的一个数据中心举行根区密钥生成仪式,生成并存储了第一个将用于互联网根区安全的密钥(KSK)。7 月 12 日,ICANN 在位于美国西部加利福尼亚州的埃尔塞贡多(El Segundo)举行第二次密钥生成仪式。7 月 15 日,ICANN 发布根区的信任锚(KSK 公钥),DNS 根服务器运营商将可以正式对根区利用实际密钥进行签名,这意味着签名根区(即应用 DNSSEC 的根区)已正式启动。根据 ICANN 的计划,根区密钥将每年生成 4 次,并且分别在位于美国东部和西部的两个中心进行,互为备份。此外,ICANN 还设置了密钥生成系统的备份机制,可以在两个中心都发生问题时进行系统恢复,重新生成密钥。

(2)顶级域部署进程加快,DNSSEC 获主要国家和地区认可

根据 ICANN 的统计[5],截至 2012 年 7 月 17 日,互联网根区记录中共有 314 个顶级域(其中包括 11 个多语种测试顶级域)。已经完成 DNSSEC 部署的顶级域占顶级域总数的 30.9%(不包含多语种测试顶级域时,比例为 28.4%)。在国家和地区顶级域方面,249 个 ASCⅡ码 ccTLD 中,已经正式运行 DNSSEC 的达到 63 个,部署但尚未完成根签的有 6 个,不仅西方主要发达国家投入运行,而且巴西、印度等发展中国家也已加入部署行列;32 个多语种国家和地区顶级域中,已完成 DNSSEC 部署的仅有 5 个,其中中国台湾的“.台湾”和“.台灣”两顶级域以及韩国的“.한국”顶级域已正式运行,斯里兰卡的两个多语种顶级域尚未完成根签。在通用顶级域方面,包括“.COM/.NET/.ORG/.INFO/.BIZ”等五大顶级域在内的 12 个通用顶级域已经正式运行 DNSSEC,在全部 22 个通用顶级域中超过半数。

(3)域名服务机构着手降低技术门槛,推动 DNSSEC 部署

为进一步加快 DNSSEC 的部署速度,域名注册管理机构和服务机构也在想尽办法降低用户使用 DNSSEC 技术的门槛。如“.EU”推出了实施自动签名的简化 DNSSEC 签名服务。通过该项服务,域名注册服务机构可按需求选择需要 DNSSEC 签名的域名,后台系统将自动完成 DNSSEC 签名服务。一些拥有部署和运行经验的域名服务机构纷纷推出 DNSSEC 解决方案和技术服务,推动二级和二级以下域名的 DNSSEC 部署进程。在各级各类域名服务机构的推动下,进入 2010 年以来,部署 DNSSEC 的区的数量出现了快速增长,几乎是呈直线上升。截至 2012 年 7 月 17 日[6],全球已有 37 191 个区能运行 DNSSEC,约为 2009 年底的 6.2 倍。捷克国家顶级域“.CZ”是 DNSSEC 部署的成功典范,目前约有 36.5%(即 34.8 万)的“.CZ”域名启用了 DNSSEC 服务,2011 年这一数字仅为 17%;预计 2012 年底使用 DNSSEC 服务的“.CZ”域名数量达到 40 万个。

3.2 DNSSEC 部署范围有望持续扩大

(1)技术特点和运行经验积累有助于加快 DNSSEC 部署

由于 DNS 所具有的树形结构和 DNSSEC 的信任机制,任何部署了 DNSSEC 的区只要使用根区 KSK 公钥进行安全认证就可以提升 DNS 解析的安全性,且 DNSSEC 已被证明是解决 Kaminsky 漏洞的长期有效方法,因此,随着根区和主要顶级域的 DNSSEC 部署完毕并投入运行,自顶向下的推动将使越来越多的域名接受 DNSSEC。而且 BIND 等主流 DNS 解析软件均支持 DNSSEC,对用户负担不重。现有解决方案在实践中不断得到检验和完善,经验的积累将进一步降低部署和运行成本。此外,域名服务机构出于经济利益的考虑也将推动域名持有人接受 DNSSEC 服务。近两年部署 DNSSEC 的区的数量大幅快速增长也显示出

这一进程正在加速之中。

(2)新通用顶级域计划将大力推动顶级域 DNSSEC 部署

ICANN 于 2011 年 6 月 20 日正式启动新通用顶级域计划,并于 2012 年 1 月 12 日—5 月 31 日接受首轮新通用顶级域申请。6 月 13 日,ICANN 公布了新通用顶级域的申请情况,共有 1 154 家机构提交了 1 930 份新通用顶级域申请。根据 ICANN 要求,新通用顶级域申请机构应具备提供 DNSSEC 服务相关的技术能力,在顶级域授权前必须通过 ICANN 有关 DNSSEC 的系统实测工作,并向 ICANN 提交测试中所用的有效密钥装置的说明文档以及顶级域的 DNSSEC 政策声明(DPS)。预计到 2015 年,将完成包括本轮次申请的新通用顶级域在内的全球绝大部分通用顶级域的 DNSSEC 的部署工作。在此带动下,全球顶级域 DNSSEC 部署速度将提速。

4 DNSSEC 的问题与不足

DNSSEC 能够较为有效地防止 DNS 欺骗,但实施 DNSSEC 尚存在一些问题[7,8]。

(1)实施 DNSSEC 是以降低 DNS 查询和响应时间性能为代价的

数据分组比原来要大得多。由于 DNSSEC 在 DNS 报文中添加了数字签名,并且密钥的长度会随着时间不断增加,因此报文长度会大大增加。考虑到 DNS 查询/应答是极为常用的互联网应用,这就会大大加重网络的额外开销,从而对网络服务的性能产生影响。

(2)实施 DNSSEC 增加了 DNS 运营和使用的负担

一方面,DNSSEC 所需密钥的产生和校验需要 CPU 计算能力作保障,但根据了解,2003 年以前生产的网络设备有不少不支持 DNSSEC,这意味着大量 DNS 运营商都需要升级其网络设备,提高 DNS 服务器配置(如将单处理器的 DNS 服务器换成多处理器的 DNSSEC 服务器)。同时,用户需要更换新版软件以改变目前 DNS 解析软件仅支持手动对 DNSSEC 进行命令行操作控制的状况。另一方面,签名和密钥占用的磁盘空间和存储器(RAM)容量将达到它们所表示数据所占容量的 10 倍。因此数据库和管理系统也不得不进行相应的升级和扩容。

(3)DNSSEC 不能提供安全有效的密钥分发通道

DNSSEC 未将通信信道的安全纳入考虑之中,目前只有借助于安全套接层(secure sockets layer,SSL)及传输层安全(transport layer security,TLS)等传输协议进行密钥分发,存在一定的安全隐患。而密钥(私钥)一旦丢失或被破解,则可能带来严重的后果。

(4)DNSSEC 会造成“安全孤岛”现象

由于 DNSSEC 不可能一夜之间部署到整个互联网,而只能逐步进行部署,因此理想情况下的信任链尚不能有效建立,DNS 与 DNSSEC 仍将并行使用,那些先部署了 DNSSEC 的区则形成一个个的“孤岛”。这会造成两种情况:第一,不安全的未签名区与签名区进行通信时会将错误信息混入其中;第二,严格执行 DNSSEC 的区会在阻止错误信息的同时将大量未应用 DNSSEC 所需的信息拒之门外。

DNS 所面临的安全威胁远不止于域名欺骗,即使部署了 DNSSEC 也绝不是在 DNS 安全方面可以高枕无忧了。对于普遍存在且造成较大危害的(分布式)拒绝服务攻击(DoS/DDoS)、对注册服务商的域名劫持、钓鱼网站等一系列 DNS 安全问题,DNSSEC 并未能提供有效解决方案。而且,由于 DNSSEC 的报文长度增加和解析过程繁复,在面临 DDoS 攻击时,DNS 服务器承受的负担更为严重,抵抗攻击所需的资源要成倍增加。

5 DNSSEC 对我国的影响及应对策略建议

DNSSEC 为互联网增加了一个新的安全手段,对我国提升 DNS 安全性提供了新的技术和思路,DNS 与 DNSSEC 并行也为我国开展研究工作留下了一定时间。但是目前全球部署 DNSSEC 的区的数量仍然较少,其实际效果究竟如何仍有待进一步观察。特别是美国主导 DNSSEC 部署进程将有助于强化其对互联网的单边控制,我国应对其可能产生的影响提前做好准备。

(1)加强技术研究和标准制定工作,积极开展试验和应用示范,积累运营和管理经验

我国作为互联网大国,境内域名和域名服务器数量都以百万计,如部署 DNSSEC 将面临大规模性能升级的技术与管理困难,在技术与产业实力较弱的情况下更多要依赖进口,支出巨大。因此,主管部门应组织有关单位,积极加大对包括 DNSSEC 在内的 DNS 安全技术的研究力度和拥有自主知识产权的 DNS 软件研发工作,设立试验环境并开展应用示范,尽早识别与解决可能出现的各种问题,为平滑升级做好技术准备;针对部署 DNSSEC 涉及的密钥产生与管理、密钥分发流程、过渡机制与互联互通等问题,推进标准制定工作,用于指导和规范相关进程,降低部署难

度与成本;对我国自主建设与自行管理的国家顶级域和未来将大量出现的新通用顶级域的 DNSSEC 部署方案进行充分研究和论证,在确保我国域名系统安全稳定运行的条件下对信任锚的可用性以及避免部署后成为“孤岛”等进行全盘考虑;针对下一代互联网、云计算、物联网、移动互联网等产业的发展可能对域名系统提出的挑战加强自主研发力度,争取提供高效、安全的域名技术,支撑新兴产业的健康发展。

(2)积极参与国际合作,扩大话语权

DNSSEC 以根区密钥作为全球域名解析安全的信任锚,这与美国单边控制的国际互联网治理框架相关。我国应在国际互联网治理的框架下统筹规划,联合有关国家,积极推动建立合理的国际互联网治理秩序,遏制少数国家对互联网关键资源的垄断,争取建立多边的、民主的全球互联网资源管理机制。同时,组织有关机构和企业以适当方式参与国际上 DNS 安全标准制定和软件开发以及密码研究工作,及时了解国际 DNSSEC 的进程与部署经验,通过多方合作,增强我国在网络与信息安全领域的硬实力与软实力。

(3)完善域名注册管理机制,保障国内域名解析安全

DNSSEC 针对 DNS 欺骗问题提出了解决方案,对增强互联网的域名安全有一定的积极作用,但是仍不能解决分布式拒绝服务攻击(DDoS)、注册端出现的域名失窃、域名劫持、钓鱼网站等大量安全问题。因此,有必要进一步健全完善互联网域名管理制度,坚持推行域名实名制注册,完善域名注册信息审核和备案流程;提高域名服务机构的管理水平和责任意识并加强监督检查,及时查处域名相关的违法犯罪行为;加强网络和信息安全的宣传教育活动,向公众普及相关知识,提高用户的自我保护意识和能力,切实保障公众注册域名所应享有的正当权益和国内的域名解析安全。

参考文献

1 毛伟. 中国互联网资源标识和寻址技术研究. 中国科学院计算技术研究所博士学位论文,2006

2 Chandramouli R, Rose S. Secure Domain Name System (DNS) Deployment Guide. NIST Special Publication (800-81r1), 2010

3 Eastlake D. Domain Name System Security Extensions. RFC 2535, March 1999

4 Chandramouli R, Rose S. Open issues in secure DNS deployment. IEEE Security and Privacy, 2009, 7(5):29~35

5 TLD DNSSEC report. http://stats.research.icann.org/dns/tld_report/,2012

6 http://secspider.cs.ucla.edu/,2012

7 李馥娟. DNSSEC 技术及应用分析. 计算机安全,2009(10)

8 蔡晨,明子鉴. DNSSEC 技术介绍与分析. 现代计算机(专业版),2010(8)

DNSSEC Technology Development and Effect Analysis

Cui Shutian[1], Liu Yue[2]

(1. Economic School of Renmin University of China, Beijing 100872, China;
2.China Academy of Telecommunication Research of MIIT, Beijing 100191, China)

Abstract This article initiates the security problems on the domain name system, analyzes the DNSSEC technology and its security performance, introduces the process of DNSSEC and the trend in the global, points out the problems and deficiencies of the DNSSEC, and finally provides the strategy suggestion on the DNSSEC deployment in China.

Key words domain name system(DNS), DNSSEC, security protection, internet governance (收稿日期:2012-08-23)