ICS 35.040
L 80

中华人民共和国国家标准

GB/T 33562—2017

信息安全技术　安全域名系统实施指南

Information security technology—Secure domain name system deployment guide

2017-05-12 发布　　2017-12-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前言 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 4
5　DNS 安全技术指南 …… 5
5.1　概述 …… 5
5.2　权威域名系统安全指南 …… 5
5.3　递归域名系统安全指南 …… 6
5.4　DNS 事务安全指南 …… 6
5.5　DNS 数据安全指南 …… 8
6　DNS 查询/响应安全指南(DNSSec 规范) …… 9
6.1　DNSSec 机制和操作 …… 9
6.2　公私密钥对的生成 …… 10
6.3　私钥的安全存储 …… 10
6.4　公钥的发布和建立信任锚 …… 10
6.5　区签名和区重签名 …… 10
6.6　密钥轮转 …… 11
6.7　创建信任链和签名验证 …… 11
附录 A（资料性附录）　具体 BIND 配置命令 …… 12
参考文献 …… 14

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:山东省标准化研究院、中国互联网络信息中心、天津卓朗科技发展有限公司、青岛以太科技股份有限公司、深圳市信息安全测评中心、深圳市坪山新区信息化管理办公室、常州富国信息技术有限公司、辽宁省信息安全与软件测评认证中心、青岛大学、青岛科技大学、互联网域名系统北京市工程研究中心。

本标准主要起草人:王曙光、王庆升、公伟、隗玉凯、姚健康、刘杰、林明贵、王伟、武刚、唐增来、邱建中、黎文辉、陶毅国、陈多思、丁锋、于佳、程相国、刘国柱、马迪。

引　言

随着网络攻击技术的发展及DNS漏洞的频繁出现，攻击者已经大大缩短了劫持DNS查找过程的任一步骤所需的时间，从而可以更快地取得对会话的控制以实施某种恶意操作。若要在长期内消除此漏洞，唯一的解决方案是以端到端的形式部署DNSSec协议，即从根区到最终域名的查找过程中每一步都部署DNSSec。

目前，作为DNSSec信任链的根服务器都已经部署DNSSec服务。与此同时，随着业界对DNSSec的努力推动，各顶级域名管理机构陆续开始部署DNSSec服务，但在顶级域名之下的二级权威域及递归域名对DNSSec支持相对较低。虽然国内重点权威域名服务器和主要递归域名服务器对DNSSec支持只有0.9%和2.2%，但它们对DNSSec支持相比以前有了较大改善。

本标准可以为域名系统DNSSec部署过程提供权威域名系统安全指南、递归域名系统安全指南、DNS事务安全指南和DNS数据安全指南等DNS安全技术指南，为DNSSec部署到各级域名系统提供技术支撑和实践指导。

信息安全技术　安全域名系统实施指南

1　范围

本标准规定了域名系统安全扩展协议(DNSSec)部署过程中权威域名系统安全、递归域名系统安全、DNS事务安全、DNS数据安全等DNS安全技术指南。

本标准适用于运行域名系统的组织内域名系统安全管理人员。

2　规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 5271.8—2001　信息技术　词汇　第8部分：安全

GB/T 5271.9—2001　信息技术　词汇　第9部分：数据通信

GB/T 25069—2010　信息安全技术　术语

GB/T 33134—2016　信息安全技术　公共域名服务系统安全要求

YD/T 2137—2010　域名系统递归服务器运行技术要求

YD/T 2138—2010　域名系统权威服务器运行技术要求

YD/T 2140—2010　域名服务安全框架技术要求

YD/T 2586—2013　域名服务系统安全扩展(DNSSec)协议和实现要求

3　术语和定义

GB/T 5271.8—2001、GB/T 5271.9—2001、GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

域名系统　domain name system

一种将域名映射为某些预定义类型资源记录(resource record)的分布式互联网服务系统，网络中域名服务器间通过相互协作，实现将域名最终解析到相应的资源记录。

3.2

名字空间　name space

一种节点与资源集合相对应的树状结构(如图1所示)。