域名系统简介及安全性分析

Introduction and Safety Analysis of Domain Name System

肖丽媛[1,2] 贺炜[1] 乔培[1]

1.西北大学信息科学与技术学院,中国·陕西 西安 710217

2.政务和公益机构域名注册管理中心,中国·北京 100088

Liyuan Xiao[1,2] Wei He[1] Pei Qiao[1]

1.School of Information and Technology, Northwest University, Xi'an, Shaanxi, 710217, China

2. China Organizational Name Administration Center, Beijing, 100088, China

【摘 要】DNS是互联网的核心基础服务,是用户访问互联网服务的必要环节,但它存在着严重的安全漏洞。论文简要介绍了DNS基本概念、安全威胁以及域名系统安全扩展(DNSSEC)基本原理。

【Abstract】DNS is the core basic service of the Internet, and it is a necessary link for users to access Internet services, but it has a serious security vulnerability. This paper gives a brief introduction to the basic concepts of DNS, the security threats and the basic principles of DNSSEC.

【关键词】域名系统;体系结构;安全分析;DNSSEC

【Keywords】domain name system; architecture; safety analysis; DNSSEC

【DOI】http://dx.doi.org/10.26549/gcjsygl.v1i3.626

1 引言

域名系统(Domain Name System,DNS)是互联网上的基础设施,是因特网的一项核心服务。DNS将域名和IP地址相互映射形成一个分布式数据库,人们不用记住IP数串,就可以更加方便地访问互联网。

2 DNS基本概念

DNS体系结构有域名空间(domain name space)、资源记录(resource record)、域名服务器(domain name server)以及解析器(resolver)4个基本要素,如图1所示。

①DNS以域名为索引,每一个域名其实是一棵很大的逆向树中的一条路径,而这棵逆向树被称为域名空间[1]。

②资源记录中存放着与域名相关的数据。资源记录被划分成不同的类(class),包括基于Chaosnet协议的网络类,使用Hesiod软件的网络类,Internet (任何基于TCP/IP协议的网络)类。资源记录包括域名、TTL(Time to live,本地域名服务器的缓存周期)、类型、类别和值5项信息[2]。常用的资源记录包括A地址、CNAME标准名称、MX邮件交换器以及NS名称服务器。A地址列出了特定主机名的IP地址,是名称解析的重要记录;CNAME标准名称用来指定标准主机名的别名;MX邮件交换器列出了负责接收到域中的电子邮件的主机;NS名称服务器指定负责给定区域的名称服务器。

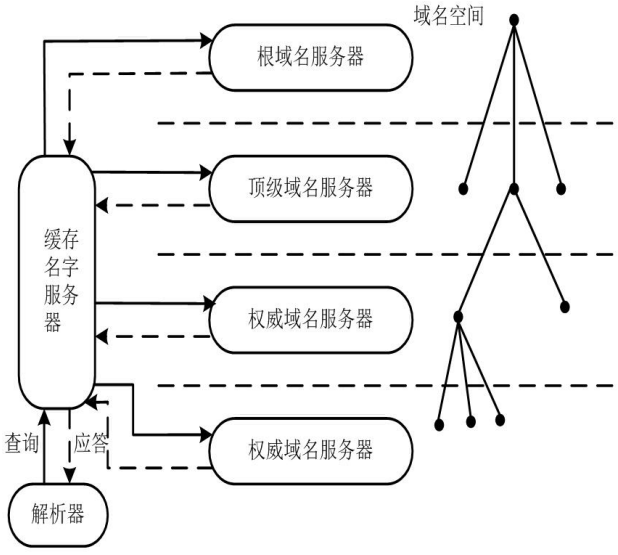

图1 DNS体系结构

③域名服务器是指保存有该网络中所有主机的域名和对应的IP地址,并具有将域名转化为IP地址功能的服务器。

④解析器是访问域名服务器的客户端程序。主机上运行的应用程序通过解析器从域名空间中获得信息。解析器处理以下任务,向域名服务器提出查询,解释响应信息、向提出请

求的程序返回信息。

域名解析是把域名解析到一个 IP 地址，然后在此 IP 地址的主机上将一个子目录与该域名绑定。进行域名解析时，客户端发送的查询消息包含 3 条内容：①指定的 DNS 域名，表示为完全限定的域名(FQDN)；②指定的查询类型，可以指定资源记录的类型或查询操作的专门的类型；③指定的类中的 DNS 域名。域名解析包括递归(recursive)解析和迭代(iterative)解析。在递归方式中，客户端有时可以使用本地缓存从上一个查询中获取的信息来回答查询。DNS 服务器还可以查询或完全解析名称，请求客户端的代表联系其他 DNS 服务器，然后发送应答返回至客户端。在迭代解析中，客户端本身可以尝试联系其他 DNS 服务器来解析名称。当客户机来执行此操作时，它使用基于服务器应答的独立和附加查询。

DNS 信息以固定的报文格式进行交互。报文格式如图 2 所示。报文由 5 部分组成：信息头、查询问题、回答、授权和额外信息。其中，信息头包括标识、标志、问题数、资源记录数、授权资源记录数和额外资源记录数。标识(2 字节)，该字段可以看作是 DNS 报文的 ID，对于相关联的请求报文和应答报文，这个字段是相同的，由此可以区分DNS 应答报文是哪个请求报文的响应。

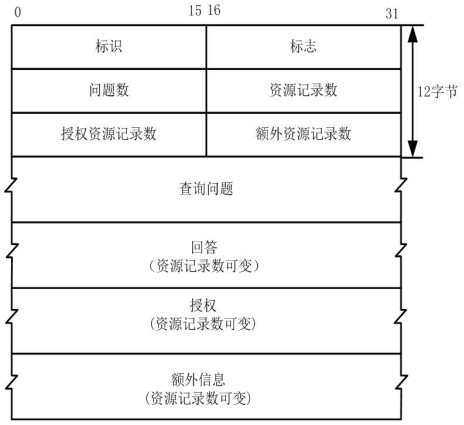

图 2 DNS 报文格式

3 DNS 安全威胁

DNS 作为 Internet 的基本支撑，缺乏适当的信息保护和认证机制。由于 Email 服务、web 访问在内的许多网络服务都与 DNS 息息相关，而 DNS 自身具有脆弱性，因此，DNS 的安全直接关系到整个互联网应用能否正常使用。近年来，针对 DNS 的攻击逐渐上升，攻击的方式主要有分布式拒绝服务攻击、域名劫持和缓存中毒等[3]。

3.1 分布式拒绝服务攻击(DDOS)

通过大量被其控制的主机或者模拟工具利用各种服务请求使被攻击的网络系统资源被耗尽，从而造成被攻击网络无法处理合法用户的请求。

3.2 域名劫持

域名劫持是互联网攻击的一种方式。采用非法手段获得某个域名管理员的账户名称和密码，或者其域名管理邮箱，然后将目标域名解析到错误的地址。域名劫持一方面影响用户的上网体验，用户被引到假冒的网站；另一方面用户可能被诱骗到冒牌网站进行登录等操作，导致泄露隐私数据。

3.3 缓存中毒

DNS 采用了缓存机制来提高查询效率。将查询过的最新记录存放在缓存中，并设置 TTL。DNS 缓存中毒则是利用了 DNS 查询的缓存机制，在 DNS 服务器的缓存中存入大量错误的数据记录并主动提供用户查询。由于攻击者的意图不同，因此缓存信息中存在特定的域名与 IP 地址的对应记录[4]。

4 DNSSEC

为了完善 DNS 的安全系统，改进和提高 DNS 的安全性能，加强 DNS 信息的认证性保护，IETF 在 1993 年提出了域名系统安全扩展（Domain Name System Security Extension, DNSSEC）的概念[5]，DNSSEC 的原理是给 DNS 应答消息添加基于非对称加密算法的数字签名来保证数据未经篡改且来源正确，再通过域名体系自下而上逐级向父域提交自己公共密钥来实现整个域名体系的逐级安全认证[6]。

5 结语

2010 年 5 月 5 日，13 台根域名服务器已经开始 DNSSEC 的升级。但是没有一种安全策略是 100%保证安全的，并且网络攻击手段层出不穷，这就要求不断提高 DNS 服务器的可靠性和安全性。服务器管理员要在实际工作中强化安全意识，从而保证用户的上网安全。

参考文献：

[1]雷迎春,龚奕利.DNS 与 BIND[M].北京:中国电力出版社,2001.

[2]李基,杨义先.DNS 安全问题及解决方案[J].电信科学,2005(02):45.

[3]方蕾等.DNS 安全漏洞以及防范策略研究[J].微电子学与计算机,2003(10):53-55.

[4]闫伯儒.DNS 安全防护平台的研究与实现[D].哈尔滨:哈尔滨工业大学,2006.

[5]李馥娟.DNSSEC 技术及应用分析[J].计算机安全,2009(1):10.

[6]蔡晨,明子鉴.DNSSEC 技术介绍与分析[J].现代计算机(专业版),2010(1):8.

基金项目：

中央编办及所属事业单位网站群系统 IPv6 升级改造项目(2012 年下一代互联网技术研发、产业化和规模商用专项)；信息安全国家标准项目(2013bzzd-WG1-006)。