DNS协议的安全浅析

The Safety Analysis of DNS Protocol

摘 要: 本文在分析了DNS协议的工作原理后，对DNS协议在Internet中的存在的漏洞进行了较详细的分析，最后提出了一些防范的措施和思路。

关键词: DNS DNS欺骗 网络安全 网络攻击

罗杰云 贺敏伟 （广东江门 五邑大学信息学院 529020）

1 引言

网络攻击的一种最主要的形式是对网络协议弱点的攻击。当初设计Internet各类协议时，几乎没有人考虑网络安全问题，网络协议或缺乏认证机制，或缺少数据保密性。因此，Internet作为TCP/IP的第五层结构，从数据链路层到应用层协议在设计上都存在不同程度的安全漏洞，可能被攻击者加以利用而入侵网络。DNS是多种Internet应用的基础，如E-mail、www、Telnet等。一旦DNS被入侵者控制，主机名及其IP地址之间的对应关系有可能被更改，从而造成主机遭受拒绝服务，或者网站被篡改等严重后果。如何保证DNS服务的安全可靠性，无疑具有深远的意义。本文从一个侧面分析了DNS协议的安全漏洞，提出了相应的防范建议。

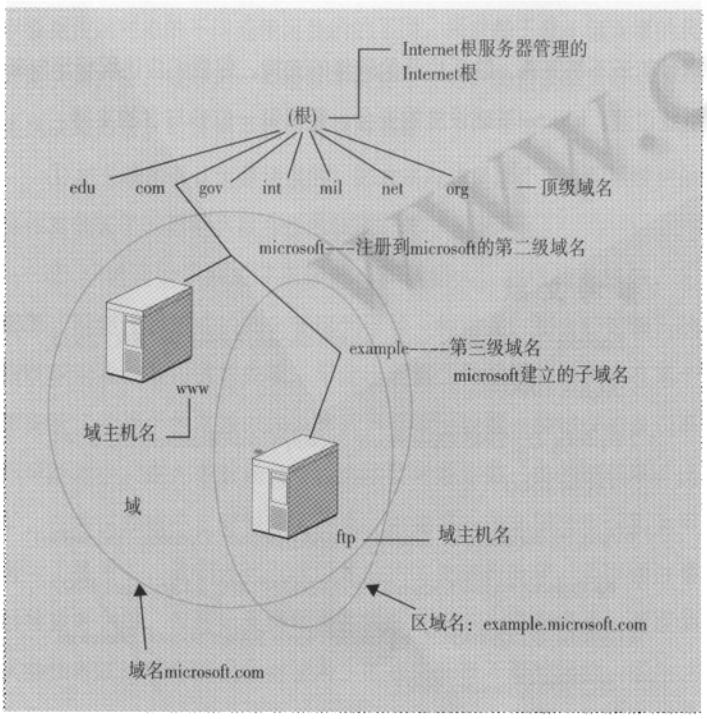

图1 域名空间示意图

2 DNS的工作原理

Internet中域名系统(domainnamesystem,DNS)是一个用于管理主机名字和地址信息的数据库系统。它将枯燥、没有意义的数字映射成具有特定含义的词或词的缩写，便于人们记忆和理解，它是Internet上一个非常重要的应用。

了解域名系统的工作原理，才能准确定位其安全漏洞所在。

2.1 域名空间

DNS的命名结构称为域名空间。域名空间是一个呈树型、层次结构分布式数据库。如图1所示。

域是域名空间的一颗子树或一个分支，树的根就是根域“”。树中最靠近根域的节点，称为Internet的顶级域(Top-level domains),每一个顶级域之下又分别包含许多级、许多个子域（subdomains）,主机则位于树的叶子上。同一级中拥有同一个父节点的标示各不相同，主机名由从相应的叶子到这一路经上的各个节点的标示组成。

域的名字就是该子树的根节点到域名空间的根节点沿途所经各个节点的标签所组成的字符串（各个标签之间用.隔开）。如：从以microsoft为根开始的子树构成一个域，他的域名为：microsoft.com。除了根域和顶级域以外，其它的域都称之为子域，子域也是相对而言的。每一顶级域之下通常包含多个子域。如：域microsoft.com是顶级域com的子域，而域example.microsoft.com是microsoft.com的子域。在DNS域名空间中，位于最下面一层的称之为域主机名，它是没有子域的，也称之为叶子（叶节点）。如上图的ftp服务器是一域主机名，它属于域example.microsoft.com下的主机，它的完全限定域名（FQDN）是ftp．Example．microsoft．com， FQDN(a fully qualified domain name)是指从域名空间根域开始的表明域的绝对位置的域名表示方法。

2.2 DNS的工作原理

域名系统的主要功能就是提供主机名和IP地址之间的对应关系。为了便于根据实际情况来分散域名管理工作的负荷，DNS实行分布式

管理的方法，各个域的域名服务器仅直接管理该节点的直接下属节点。DNS由解析器、名字服务器和资源记录组成。DNS的客户端称为解析器（resolvers），它通常作为库例程存放，供需要使用名字服务的应用程序引用，解析器负责组织查询信息并发送给服务器。存储关于域名空间信息的程序叫做名字服务器（name server）。名字服务器通常含有域名空间中某区域的资源记录，名字服务器负责维护本区域的资源记录，缓存其它区域的资源记录，为解析器提供查询答案或更接近目标的DNS服务器地址。DNS数据库文件中的大部分条目被称为DNS资源记录（resource record，RR）。各个资源记录标识的都是数据库中的某个资源，它记录域名解析的有关信息，如主机名机器IP地址之间的对应关系，主要有以下几种类型：

地址（A）资源记录：该记录维护了名字到IP地址的关联。地址解析时，服务器取出与主机名匹配的A记录，将此记录中的IP地址作为响应。

SOA资源记录：SOA（Start of Authority,起始授权）记录包括很多配置内容和服务器信息，如所在域、授权服务器、管理员e-mail地址、序列号、资源记录类型等。每个区域都包含一个SoA资源记录。SOA记录标识了全局DNS数据库的划分（也称为分区）的上界。每个配置文件都必须包括一个SOA记录，以标识服务器所管理的数据库的起始地方，

名字服务器（NS）资源记录：NS（Name Server,运行DNS服务的服务器）资源记录将DNS层次结构连接到一起。一个NS记录定义了哪个名字服务器负责哪个区（或子域）。它可以向子域的服务器指出其父域服务器。每个区域必须在根域中至少包含一个NS资源记录。

指针（PTR）记录：指针(PoinTer Record)记录用来将IP地址映射成主机名。以提供从IP地址到主机名映射的反向搜索。

邮件交换（MX）记录：一个MX（Mail eXchange）记录指明了域名所对应的邮件服务器。邮件服务器负责处理或转发此域中的邮件。

正规名字（CNAME）记录：一个CNAME(Canonical Name)记录定义了主机的别名,可以用来向用户隐藏网络工作的细节，或是减少域名更动影响。

从DNS服务器获取数据的过程称为名字解析。DNS解析有两种方式：迭代(iterative)和递归（recursive）。在迭代方式中，如果服务器查找不到对应的记录，会返回另一个可能知道结果的服务器的IP地址给查询的发起者，以便它向新的DNS服务器发送查询请求。在递归方式中，当客户向DNS服务器提出请求之后，此服务器就负责查询出相应记录，如果不能从该服务器本地得到解析，由该DNS服务器向其他DNS服务器发出请求，直到得到查询结果或出现超时错误为止，相当于由收到递归请求的DNS服务器来完成迭代查询中用户的工作。

域名查询的解析过程，忽略了各个国家及地区地理位置的差异,按照分层结构的特点自上而下进行。以主机cs.wyu.edu.cn查询主机www.sina.com.cn的IP地址为例,该例采用迭代方式查询，其说明过程如图2所示。主机cs.wyu.edu.cn首先把查询请求发送给本地DNS服务器，本地DNS服务器收到请求并在本地数据库中查找记录，如果找不到对应记录，则本地DNS服务器向自己的根域服务器发出迭代查询请求；若根域服务器无法解析,则返回管理cn域的DNS服务器的IP地址。;本地DNS服务器又把请求交给管理cn域的DNS服务器；若管理cn域的DNS服务器无法解析,管理cn域的DNS服务器返回管理com.cn的DNS服务器的IP地址；本地DNS服务器再把问题交给管理com.cn的DNS服务器，若管理com.cn域的DNS服务器无法解析；管理com.cn域的DNS服务器返回sina.com.cn名字服务器的地址；最后本地名字服务器从sina.com.cn名字服务器获得地址,并将结果返回给客户解析器.

注:解析顺序从（1）到（10）.

（1）、（2）、（4）、（6）、（8）为查询www.sina.com.cn的请求;

（3）返回cn名字服务器地址;

（5）返回com.cn名字服务器地址;

（7）返回sina.com.cn名字服务器地址;

（9）、（10）返回www.sina.com.cn的IP地址。

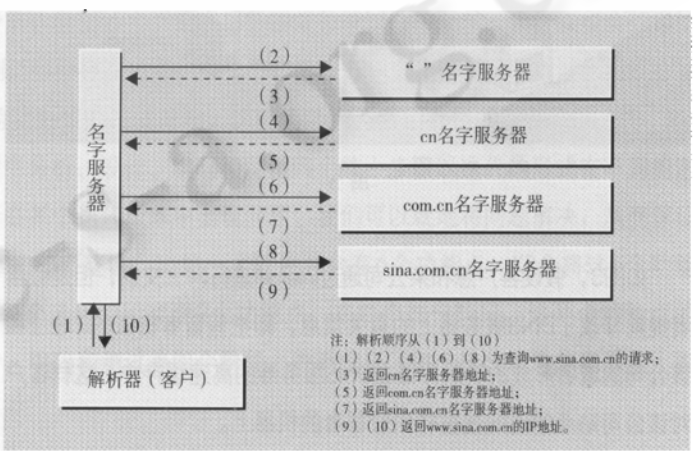

图 2　DNS 的解析过程

3 DNS 安全脆弱性分析

脆弱性是指容易被利用而危及安全的一种境况，比如导致非授权访问或使用系统，它是一种潜在的导致安全性被破坏的可能性。下面我们从系统设计、软件实现、使用配置等方面来分析DNS所存在的安全漏洞。

在系统设计方面，DNS的设计受到当时技术水平、设计目标等因素，没有提供认证机制，查询者在收到应答时无法确认应答信息的真假，这样很容易导致欺骗。攻击可以用简单的方法探测域名服务器查

询信息的ID，伪造虚假的应答报文，并使之在真正的应答之前到达，从而给出虚假的主机名和IP的映射关系或者虚假的域名服务器信息，这种DNS欺骗，可能把用户导向为入侵者所控制的站点，从而为用户提供伪造的页面，发布伪信息，或造成站点被修改的假象；或者通过在目标机上假造用户所熟悉的界面而骗取用户输入的敏感数据；可能使入侵者假借被信任主机的身份而侵入系统内部（使被信任的主机与攻击者控制的主机IP相对应）；DNS的一个基本特性是使用超高速缓存，即当一个名字服务器收到有关映射的信息（主机名字到IP地址）时，它会将该信息存放在高速缓存中。这样若以后遇到相同的映射请求，就能直接使用缓存中的结果而无需通过其他服务器查询。这种映射表是基于高速缓存，动态更新的。这是DNS在设计上的特色之一，但也是安全问题之一。由于正常的映射表的刷新都是有时限的，这样假冒者如果在下次更新之前成功地修改了DNS服务器上的映射缓存，就可以进行DNS欺骗或者拒绝服务攻击了。

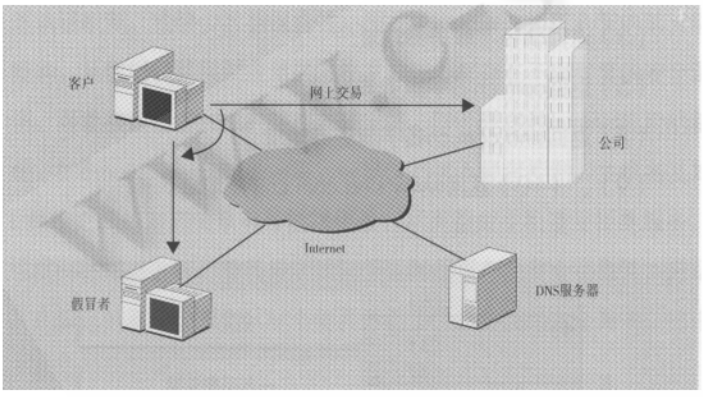

图 3

如图3，假设客户想和某公司通过Internet进行网上交易，但是假冒者提前修改了DNS服务器上的有关信息，即把假冒者机器的IP地址和该公司的域名形成的映射存储在DNS服务器的高速缓存中，这样客户对该公司站点的访问就被转到假冒者的机器上。

所有的大型复杂软件系统，实现DNS系统功能的软件，比如BIND（Berkeley Internert Name Domain）是我们所熟知的域名软件，它具有广泛的使用基础，Internet上的绝大多数DNS服务器都是基于这个软件的，该软件自从投入使用以来，新版本、新BUG的交替出现一直持续不断。来自DIMAp/UFRN（计算机科学和应用数学系/北格兰德联邦大学）的CAIS/RNP(Brazilian Research Network CSIRT)和Vagner Sacramento对BIND的几种版本进行了测试，证明了在BIND版本4和8上存在缺陷，攻击者利用这个缺陷能成功地进行DNS欺骗攻击。

配置上的疏忽也会导致安全上的缺陷。为了系统的容错性，通常在域名服务器中，除了设置主服务器之外，还会设有夫名服务器，当主域名服务器出现故障时，辅服务器可以行使主域名服务器的职能。为了有效维护主、辅服务器的域名数据之间的一致性，域名系统设有"域传送"（zone tranfer）功能，使查询者通过简单的查询获得域服务器所维护的本地数据信息，包括本域所有的主机名和IP地址的对应信息、有关主机、Mail服务器信息等。然而，如果这种方法被滥用，则可能把内部信息暴露给企图入侵者。从而入侵者了解内部设备运行的软件有关信息，根据所掌握的安全漏洞报告，锁定入侵的切入点，为其进一步入侵提供了便利。

4 DNS的安全保护

从前面的分析，我们可以了解，一旦域名服务器被入侵者控制，有可能造成信息泄露、关键资源被侵入、拒绝服务等严重后果，因此有必要加强我们对基础设施的保护意识。对于系统的设计及其软件实现中的安全性，绝大多数的最终用户无法直接参与，因此，必须紧密跟踪有关组织给出的安全问题报告，及时升级、更新软件系统。而系统配置、使用由每一个系统管理人员直接参与，原则上，任何应用系统都有可能被配制成为不安全，所以，保护域名服务器，更要严格系统配置。通过适当的配置，隐藏BIND软件的版本号，以阻止入侵者轻易找到相应的版本上的漏洞；配置区域转送时，严格控制区域传送，以防止入侵者通过正常的系统查询命令获得丰富的内部信息；在配置named.conf时,可以采取allow-transfer控制来加强安全。

使用交叉检验，即服务器通过反向查询已得到IP所对应的主机名之后，再用该主机名查询DNS系统对应于该主机名的IP地址。如果两者一致，就说明该客户合法，否则，就是非法。如果攻击者仅改变了名字查询或反向查询所依赖的多个文件中的一个，这种方法可以发现对应关系不一致，从而使DNS欺骗无效。

防火墙是最常用的安全产品之一。借助防火墙，在设置好的防火墙的前后各设置一个DNS服务器，即内、外DNS服务器。在内部网络中设置内部DNS服务器，内部DNS服务器提供内部网名字域到保留IP地址的解析，只能由内部网的主机使用，对Internet主机不可见，即不在上级DNS服务器登记。对内部网名字域外的Internet域名解析的任务直接提交给外部DNS服务器完成。在DMZ区中设置对外的外部DNS服务器。外部DNS负责提供外部用户的查询，同时处理来自内部DNS服务器提交的请求。这样也简化域名服务器安全管理。

要从根本上改进DNS的安全性，需要从修正系统设计着手，提供必要的信息认证机制，阻止DNS欺骗。IETF的域名系统安全工作组，已经提出了关于域名系统安全扩展（DNSSEC）的一系列的建议方案，主要设想是在兼容现有协议的基础上，引入加密/认证体系，每一区

下转第 35 页 >>

（zone）都有一对区级的密钥对，密钥对中的公钥用于对区中的域名记录信息做数字签名，从而使支持DNS安全扩展的接收者得以检验应答信息的可靠性。

DNSSEC的安全性虽然有所提高，但目前存在许多难以解决的问题。首先是系统效率问题，生成或者检验签名信息都会耗费系统资源，算法越复杂，密钥越牢靠（越长），需要签名或检验的记录越多，消耗的资源就越多。提供同样的服务，支持DNSSEC的服务器对设备性能的要求将会更高。其次是密钥系统的管理问题，包括密钥的分发、保存、更新以及废除等，目前还没有完美的解决方案。所有的这些问题有待于进一步的探讨。

5 结束语

本文对DNS的工作原理进行了阐述，分析了DNS的安全漏洞源于系统的设计、实施和配置等方面，同时指出了保证DNS安全的一些措施。DNSSEC————DNS的安全扩展是最具吸引力的解决方案，尽管目前还不甚完善，缺乏广泛的软件的支持，但我们应该积极地向新系统过渡。Internet基础设施的安全，需要每一位参与者的支持。

参考文献

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

2 Eastlake, D., "DNS Operational Security Considerations",RFC 2541, March 1999.

3 Vixie, P., Thomson, S., Rekhter, Y. and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)", RFC 2136, April 1997.

4 Eastlake, D., Kaufman, C., "Domain Name System Security Extensions", RFC 2065, January 1997.