DNS域名系统的安全性分析

杭州师范学院计算机系　姚茂群

为了使信息相互正常传送，Internet上的每一台机器都必须拥有属于自己的IP地址，由于IP地址难于记忆和识别，为方便使用，在实际网络应用中，通常使用集中式资源命令工具——域名系统（DNS）。

一、DNS域名系统简介

DNS(Domain Name Server)是Internet用于名字登记和解析的标准，任何IP地址均可以由字母组成的名字代替，DNS作为一个分布式数据库，它的主要任务是将一组名字分散至各个域，每个域负责整个域中名字的一个子集，并可以再建子子域，这种层次结构如同一棵倒立的树，最高的域为根域，根下面是一级域，例如按照地理位置每个国家及地区设立一个一级域，由两个字母作为域名，如中国以cn表示，英国以uk表示。每个一级域又可以建立相应的二级和三级域等。主机名字由自下而上直到一级域的各级域名构成，每一级域名之间以“.”作为分隔符，例如：aaa.bbb.ccc.uk。每个域有一个名字服务器，该名字服务器的数据库中除了存有它所能负责的下级域的IP地址转换信息外，还能为继续搜索域名空间以便找到不属于它负责范围内的域名提供有关信息。当需要将主机名字转换成地址时，就向DNS名字服务器发送正向地址查询请求，当需要将地址转换成名字时，就向DNS名字服务器发送反向地址查询请求，名字服务器可根据数据库中所保存的数据给予答复。

例如：主机ccc.cn正向查询www.aaa.bbb.uk的IP地址的解析过程如下：

(1)主机ccc.cn把查询www.aaa.bbb.uk的IP地址的请求发送给负责ccc.cn的本地名字服务器，即cn名字服务器。因为本地服务器不是域www.aaa.bbb.uk的权威主人，无法提供权威答复，便向某根名字服务器转发同样的请求。

(2)根名字服务器接收到请求后，答复它所负责的uk名字服务器的IP地址。本地服务器得到该答复后，便把查询www.aaa.bbb.uk的IP地址的请求转发给uk名字服务器。

(3)uk名字服务器接收到该请求后，答复它所负责的bbb.uk名字服务器的IP地址。本地服务器得到该答复后，便把查询www.aaa.bbb.uk的IP地址的请求转发给bbb.uk。

(4)bbb.uk名字服务器接收到该请求后，答复它所负责的aaa.bbb.uk名字服务器的IP地址。本地服务器得到该答复后，便把查询www.aaa.bbb.uk的IP地址的请求转发给aaa.bbb.uk。

(5)aaa.bbb.uk名字服务器接收到该请求后，答复它所负责的www.aaa.bbb.uk名字服务器的IP地址。本地服务器得到该答复后，便把该地址转交给主叫的主机ccc.cn，至此，主叫主机和被叫主机便可进行通信了。

二、域名系统的安全性分析

由于许多UNIX的应用是以主机名作为访问控制表的基础，因此，如果DNS名字服务器为攻击者所控制，则系统安全将受到极大威胁。DNS欺骗是攻击者的主要手段。攻击者设法提供一个错误的域名，当系统进行认证时，就以此欺骗系统实现非授权访问的目的。一般的攻击者可以通过以下两种方法来实施DNS欺骗。

1.修改IP地址表

攻击者设法取得DNS名字服务器的信任之后，尽管无法准确预测DNS客户要向哪一个地址发出查询请求，但可以假定某个比较流行的网络名称或者以攻击者个人的选择来取代所有的地址，从而改变主机的IP地址表，并将修改后的IP地址表存入DNS名字服务器的转换数据库中。当客户发出查询请求时，他就会得到一个虚假的、并已为攻击者所控制的IP地址。

2.利用高速缓存

DNS名字服务器的高速缓存是影响DNS域名系统安全的重要因素。攻击者可利用某个程序缺陷或配置上的错误等安全漏洞，将错误信息存入高速缓存。由于错误信息可在高速缓存中保留相当长的时间，所以这些错误信息将会误导查询结果，而误导查询的响应也同样会被高速缓存。此外，由于DNS名字服务器除了响应查询信息外，还可提供附加信息，假如攻击者提供了虚假的附加信息，则这些信息也将被查询它的名字服务器高速缓存，也就是说，受到破坏的名字服务器会导致未受到破坏的名字服务器高速缓存错误信息。利用上述安全弱点，攻击者可实施DNS欺骗。假设攻击者已经控制了某台名字服务器，当有查询申请时，该名字服务器就会提供权威响应，权威响应将指示客户机查找与之相连的服务器的名字，如果攻击者利用名字服务器的高速缓存，将其控制的服务器的名字写入高速缓存，则客户机得到的是攻击者控制的服务器的名字，而不是客户真正想要连接的合法服务器的名字。同样道理，

伪造的反向地址查询又可欺骗服务器确定非授权用户的IP地址的合法性。

例如：假设现有A公司域名为aaa.com、B公司域名为bbb.com、C公司域名为ccc.com。其中B公司已为攻击者所控制。现在，A公司职员张三通过Web浏览器访问bbb.com中的某个站点，于是浏览器向A公司名字服务器发出的DNS查询经其转发传给B公司名字服务器，B公司名字服务器的响应信息，诸如所请求的站点的IP地址及附加信息全部被存入A公司名字服务器的高速缓存。由于B公司名字服务器已被攻击者所控制，所以攻击者可以将错误信息引入附加信息域，比方说：引入C公司域名ccc.com负责范围内的某个域名ddd.eee.ccc.com以及攻击者可控制的另外一台机器D的IP地址。与此同时，如果A公司的另一名职员李四正巧远程登录ddd.eee.ccc.com，则Telnet将向A公司名字服务器发出DNS查询请求，A公司名字服务器接到该查询请求之后就会把高速缓存内存在的错误信息包括ddd.eee.ccc.com域名及另外一台为攻击者所控制的机器D的IP地址作为响应答复李四的机器。于是，李四的机器与机器D建立了连接，而攻击者再用其所控制的机器D与域名为ddd.eee.ccc.com的机器建立连接。李四象往常一样输入用户名和密码之后，即可完成登录，而事实情况是：李四实际连接的真正机器是高速缓存中的IP地址所指示的、为攻击者所控制的机器，李四在显示器上所见到的也是由攻击者提供的伪造登录符，攻击者实际利用了A公司名字服务器的高速缓存，将自己的机器D置于李四的机器和域名为ccc.com的主机之间，这样，李四的机器与C公司之间传送的所有信息都将经过攻击者的机器D，并为他所控制，遗憾的是，李四却往往毫无查觉，这就是DNS欺骗。

三、检测与防范DNS欺骗的方法

检测与防范DNS欺骗的方法主要有以下几种：

1. 交叉检查查询的响应

所谓交叉检查即服务器通过反向查询向DNS系统询问某个预期客户的IP地址所对应的DNS名字，再用该名字查询DNS系统对应于该名字的地址。如果两者一致，就说明该客户合法，否则就是非法。但是这种技术也有局限性，由于地址信息表保存在多个单独文件中，这些文件有可能位于不同的名字服务器，如果攻击者只改变了对应于反向查询的名字服务器文件而没有改变对应于正向查询的名字服务器文件，则交叉检查可以检测DNS欺骗，如果攻击者同时修改正向和反向地址信息表，则交叉检查将不起作用。

2. 使用软件

限制高速缓存错误信息扩散的方法是运行名字服务器软件。使用BIND程序来控制对DNS名字服务器的查询发送，对有疑问的站点，可以使用bogusns指令来防止查询发送。也可以增加对名字服务器的检查，使其只响应选择的客户而不是所有客户。

如果怀疑某台主机受到DNS欺骗攻击，可另选网络中已经授权主机作为DNS服务器，如果攻击者入侵第一台主机时间不久，则可通过比较其他授权服务器与被攻击的DNS服务器的路由地址表来作判断。如果比较结果相同，则说明被怀疑的主机未受到DNS欺骗攻击。如果比较结果不相同，则说明被怀疑的主机确实受到DNS欺骗攻击。如果攻击者控制该服务器时间相当长，则伪造的主机地址可能已经传遍了整个网络上的所有DNS服务器，此时上述方案已无法检测出DNS欺骗，可选用检测域中不正常行为的DOC脚本程序，DOC可向被测的DNS服务器发送请求，然后再对接收到应答后的输出进行分析。

3. 设置防火墙等

在设置好的防火墙前后分别运行一个名字服务器，防火墙前的名字服务器包括网关的名字和IP地址，防火墙后的名字服务器包括内部主机的全部名字和IP地址，并将两个名字服务器用静态路由耦合以阻止错误信息进入防火墙后的名字服务器。

此外，如果名字服务器运行在一台普通用户使用的机器上，则一定要保证/etc/named.boot中指出的所有文件为boot所有，确保这些文件的安全。在条件允许的情况下，可将名字服务器设置在一台特定的无用户帐户的机器上。甚至有时，为了进一步保护自己，可使用IP地址，而不用主机名称。有些操作系统引入名字到地址及地址到名字的映射来简化DNS，以增加安全性。

参考文献

[1] http://www.cs.purdue.edu

[2] http://www.cs.princeton

[3] http://www.isc.org

[4] Simson Garfinkel , Gene Spafford. Practical Unix & Internet Security. 电子工业出版社，1999