防范DNS欺骗的策略

李 涵,罗新华

(河南师范大学 计算机与信息技术学院,河南 新乡 453007)

摘 要:分析了DNS协议的工作原理后,对DNS协议在Internet中欺骗的实现进行了较详细的分析,最后提出了一些监测和防范的措施。

关键词:DNS;DNS欺骗;数字签名

中图分类号:TP309.2 **文献标识码**:A **文章编号**:1672-7800(2008)10-0177-02

1 DNS欺骗的定义及其原理

DNS(Domain Name Server)是指域名服务器,而DNS欺骗就是攻击者冒充域名服务器的一种欺骗行为。

DNS解析有两种方式:①interative迭代。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,以便它向新的服务器发起查询请求。②recursive递归。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服务器向其它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。

结合DNS服务器工作的方式,攻击者可以冒充域名服务器,然后把查询的IP地址设为攻击者的IP地址,这样的话,用户上网就只能看到攻击者的主页,而不是用户想要取得的网站的主页了,这就是DNS欺骗的基本原理。DNS欺骗其实并不是真的"黑掉"了对方的网站,而是冒名顶替、招摇撞骗罢了。

2 DNS欺骗的实现

2.1 DNS高速缓冲存储器麻痹(DNS Cache Poisoning)

可以想象,DNS服务器不可能将所有现存的域名或IP地址存储在本身的存储空间里。这就是为什么DNS服务器有一个高速缓冲存储器(cache),它使得服务器可以存储DNS记录一段时间。事实上,一台DNS服务器只会记录本身所属域中的授权的主机,如果它想要知道在自身域以外主机的信息,就必须向信息持有者(另一台DNS服务器)发送请求,同时,为了不每次都发送请求,这台DNS服务器会将另一台DNS服务器返回的信息又记录下来。

现在,用一具体事例来说明攻击者如何实现麻痹DNS缓存。假设攻击者有自己的域(invasor.net)和一个已被攻陷的DNS服务器(ns.invasor.net)。攻击者已经自定义了其DNS服务器的记录,比如,记录可以是www.sina.com=172.40.40.40。则有如下步骤:①攻击者向DNS服务器发送请求查询www.invasor.net;②目标DNS服务器不知道这台主机的IP地址,因为它不属于本身域,所以目标DNS服务器就会询问此主机的所属域的DNS服务器;③这时被黑DNS服务器就会回复目标DNS服务器,在此同时它也会给出它所有的记录,这个过程叫做zone transfer;④这时目标DNS服务器还没有被麻痹。攻击者得到了自己的IP地址,但是他的目标是逼迫zone transfer进行以使目标DNS服务器麻痹直到其缓存不会被清除或更新;⑤现在如果再询问目标DNS服务器关于www.sina.com的IP地址,它会告诉你172.40.40.40,这也正是攻击者的服务器所在。现在,攻击者就能为所欲为了。

2.2 DNS ID欺骗(DNS ID Spoofing)

当主机X要与主机Y联系时需要有Y的IP地址。然而在绝大多数情况下,X只有Y的名字,这样,DNS协议就是来解决名字到IP地址的问题的。因此,X就会向它所在域的DNS服务器询问Y的IP地址。其间,主机X分配一个随机数,这个数也将会出现在从DNS服务器返回的信息里。当X收到回复后,X会对比两个数字,如果一致,则收到信息被视为有效。

因为DNS协议的提出请求是依赖于UDP的(只有在zone transfer时才用TCP),所以没有SYN/ACK号,这也就意味着发送一个伪造的包是极其简单的。

攻击者用嗅探器拦获ID,回复构造过的包给受害主机。但即使攻击者拦截了请求,数据包还是会传去DNS服务器,而DNS服务器也照样会回复(除非攻击者拦截并阻止对网关的请求或实施ARP缓存麻痹才可能在转换网络中攻击)。这就意味着攻击者必须在真DNS服务器前回复,即为了攻击成功,攻击

作者简介:李涵(1987~),男,河南开封人,河南师范大学计算机与信息技术学院本科生,研究方向为计算机网络通信;罗新华(1987~),男,湖南常德人,河南师范大学计算机与信息技术学院本科生,研究方向为无线网络及网络安全。

者必须和被攻击者在同一个LAN,只有这样他才可以获得快速的ping并且捕获对方的数据包。

3 DNS欺骗防范方法

3.1 DNS服务器冗余

在网络工程的设计与数据库的维护中,为了保证整个网络和数据的稳定性和抗突发事件的能力,避免存在单点故障的危险,一般都对关键设备或数据进行"备份",即设备在Internet中的冗余性。借助于这种"备份"思想,我们可以在一定的程度上降低DNS欺骗的发生。

对于每台接入Internet的计算机来说,在具体的某一时刻都有一台DNS服务器为它提供域名解析服务。然而,实际上该网络中可能存在着类似的、满足要求的其它服务器可以为该计算机提供服务。如图1所示。

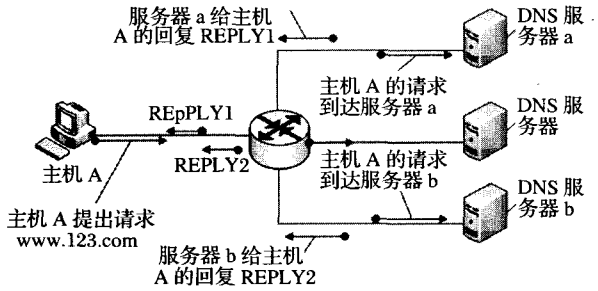

图1 利用服务器冗余防范攻击

现有主机A欲发送请求查询www.123.net,服务器a和服务器b分别收到请求后,依据自身已存储的内容或是通过查询其它服务器的方式获得与域名www.123.net相对应的IP地址,然后返回给主机A。

当主机A接收到第1个REPLY(不妨假设来自于服务器A)后,暂且忽略REPLY中信息的正确性,存储下REPLY1中的信息并按照REPLY1中的信息来完成访问www.123.net的动作。

当接收到第2个REPLY之后,主机A便将收到的两个REPLY中包含的信息进行对比,如果两个REPLY中返回的www.123.net的服务器的IP相同,而且发送这两个REPLY报文的主机的IP地址不同,则可以证明此台计算机未受到欺骗。否则,如果返回www.123.com的IP地址不同或是返回的与域名www.123.com相对应的IP地址相同,而且返回的服务器A和B的IP也相同,就表明为该计算机提供服务的DNS服务器受到攻击,此时主机A可以采取相应的应对措施防止损失进一步扩大。如果某用户对服务质量要求很高,可以一定程度上继续增加DNS服务器的数量,这样就可以提高对DNS欺骗的监测力度,提高服务质量。

3.2 静态MAC绑定

DNS欺骗是通过改变或冒充DNS服务器的IP地址,所以可以采用MAC地址和IP静态绑定来进行防范,因为每一张网卡的MAC地址是唯一的,将DNS服务器的MAC地址与其IP地址绑定,并存放在网内主机网卡的EPROM中,当主机每次向DNS发出请求后,便检查DNS服务器应答中的MAC地址是否与保存的MAC地址一致,如果不一致,就说明该区域的DNS服务器遭到攻击。但此方法也有一定的缺陷,如果是局域网内部的主机,仍可以进行DNS欺骗,因为它也保存了DNS服务器的MAC地址,所以此方法具有一定的局限性。

3.3 设置数字密码鉴别

在域文件数据的传输过程中,为了防止出现意外,可以设置任务数字签名(TSIG)。在主从域名服务器中设置相同的密码和算法。要求传输通讯时予以鉴别和确认。由于有密码认证,使得主从服务器的身份难以伪造。增强了域名数据传输的可靠性。

更强有力的可靠域名服务是利用DNS安全扩展(DNSSEC),用数字签名的方法对查询中的数据源进行鉴别,对数据完整性进行检查。DNSSEC的规范可参考RFC2605。由于在建立域时就要生成加密密码,并且要求上级域名也要完成相应的域密码签名,过程比较的繁琐。InterNIC域名管理至今未采用。但是从理论上看,DNSSEC应当是可靠的域名建立和解析方法。对防止域名欺骗等行为是有效的。

3.4 优化DNS服务器设置

不管您使用哪种DNS,请遵循BlueCat Networks公司总裁Michael Hyatt提供的以下最佳惯例:①在不同的网络上运行分离的域名服务器来取得冗余性;②将外部和内部域名服务器分开(物理上分开或运行BIND Views)并使用转发器(forwarders)。外部域名服务器应当接受来自几乎任何地址的查询,但是转发器则不接受。它们应当被配置为只接受来自内部地址的查询。关闭外部域名服务器上的递归功能(从根服务器开始向下定位DNS记录的过程)。这可以限制那些DNS服务器与Internet联系;③可能时,限制动态DNS更新;④将区域传送(zone transfer)限制在授权设备上;⑤利用事务签名对区域传送和区域更新进行数字签名;⑥隐藏服务器上的BIND版本;⑦删除运行在DNS服务器上的不必要服务,如FTP、telnet和HTTP;⑧在网络外围和DNS服务器上使用防火墙服务。将访问限制在那些DNS功能需要的端口上。

4 结束语

本文对DNS解析及DNS欺骗的原理进行了阐述,分析了DNS存在的一些安全问题,同时指出了保证DNS安全的一些措施,对维护DNS服务器的安全具有一定的参考意义。

参考文献:

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

[2] MOCKAPETRIS P.Domain names -Concepts and Facilities,RFC 1034[S].1987.

[3] 罗杰云.DNS协议的安全漏洞及其防范浅析[J].福建电脑,2003(8).

[4] 孙永兴,邵庆东,李斌,等.建立安全可靠的DNS系统[J].计算机工程,2000(26).

(责任编辑:王 钊)