DNS 欺骗攻击及其防护研究

王 伟

(西安财经学院 信息与教育技术中心,陕西 西安 710100)

摘 要:DNS是计算机用户访问网站使用的域名地址解析系统。DNS欺骗则是攻击者常见的攻击手段。从DNS的服务工作过程入手,分析了DNS的欺骗原理,探讨了防止DNS欺骗攻击的技术方法。

关键词:DNS;欺骗攻击;防护研究

中图分类号:TP309 文献标识码:A 文章编号:1672-7800(2012)003-0138-03

0 引言

域名系统(Domain Name System,DNS)是一个将Domain Name和IP Address进行互相映射的Distributed Database。DNS是网络应用的基础设施,它的安全性对于互联网的安全有着举足轻重的影响。但是由于DNS Protocol在自身设计方面存在缺陷,安全保护和认证机制不健全,造成DNS自身存在较多安全隐患,导致其很容易遭受攻击。很多专家就DNS Protocol的安全缺陷提出了很多技术解决方案。例如IETF提出的域名系统安全协议(Domain Name System Security,DNSSEC),其目标就在于解决这些安全隐患。这个Protocol增加了安全认证项目,增强了Protocol自身的安全功能。但是新增加的安全机制需要占用更多的系统和网络资源,同时要升级Database和System Manggament Software,这些基于DNSSEC协议的软件还不成熟,距离普及应用还有较长时间。目前,常见的措施是定期升级DNS软件和加强相关的安全配置,禁用不安全的端口等。本文对以侦听为基础的DNS ID欺骗(DNS ID spoofing)进行了探讨,并提出了相关的防护解决方案。

1 DNS SERVER的服务工作过程

DNS是一种实现Domain Name和IP Address之间转换的系统,它的工作原理就是在两者间进行相互映射,相当于起到翻译作用,所以称为域名解析系统。DNS System分为Server和Client两部分,Server的通用Port是53。当Client向Server发出解析请求时,Local DNS Server第一步查询自身的Database是否存在需要的内容,如果有则发送应答数据包并给出相应的结果;否则它将向上一层DNS Server查询。如此不断查询,最终直至找到相应的结果或者将查询失败的信息反馈给客户机。如果Local DNS Server查到信息,则先将其保存在本机的高速缓存中,然后再向客户发出应答。日常我们上网是通过Browser方式来申请从Domain Name到IP Address的解析,即Client向DNS Server提交域名翻译申请,希望得到对应的IP Address。这里以笔者所在院校为例,说明DNS的工作原理。

例如Client的Address为10.252.2.16,学校DNS Server为218.30.19.40,从此客户机来访问西安财经学院网站。在地址栏键入学校网站的www.xaufe.edu.cn,通过DNS Server查找其对应的IP Address。这个申请从10.252.2.16的一个随机PORT发送出去,由218.30.19.40的53绑定端口接收到此申请并进行翻译,首先在218.30.19.40的高速缓存中查找www.xaufe.edu.cn的IP Address,若存在对应的映射关系,就直接将IP Address发送给客户机,若缓存中没有,则218.30.19.40会向上层DNS SERVER查询,最后将查询到的结果先发送到218.30.19.40,最后由218.30.19.40将西安财经学院的IP Address(281.195.32.1)返回给Client 10.252.2.16。这样10.252.2.16就可以和西安财经学院站点建立连接并访问了,其具体过程如图1所示。

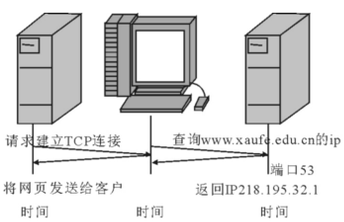

图1 客户端Browser向DNS查询Web服务器的IP地址

作者简介:王伟(1978-),男,山西新绛人,硕士,西安财经学院信息与教育技术中心工程师,研究方向为计算机信息系统、网络管理与安全。

2　DNS 欺骗攻击原理

2.1　欺骗原理

Client 的 DNS 查询请求和 DNS Server 的应答数据包是依靠 DNS 报文的 ID 标识来相互对应的。在进行域名解析时,Client 首先用特定的 ID 号向 DNS Server 发送域名解析数据包,这个 ID 是随机产生的。DNS Server 找到结果后使用此 ID 给 Client 发送应答数据包。Client 接收到应答包后,将接收到的 ID 与请求包的 ID 对比,如果相同则说明接收到的数据包是自己所需要的,如果不同就丢弃此应答包。根据攻击者的查询和应答原理,可使用不同方法实现攻击,如:

(1)因为 DNS Message 仅使用一个简单的认证码来实施真实性验证,认证码是由 Client 程序产生并由 DNS Server 返回结果的,客户机只是使用这个认证码来辨别应答与申请查询是否匹配,这就使得针对 ID 认证码的攻击威胁成为可能。

(2)在 DNS Request Message 中可以增加信息,这些信息可以与客户机所申请查询的内容没有必然联系,因此攻击者就能在 Request Message 中根据自己的目的增加某些虚假的信息,比如增加其它 Domain Server 的 Domain Name 及其 IP Address。此时 Client 在受到攻击的 Domain Server 上的查询申请均被转向此前攻击者在 Request Message 中增加的虚假 Domain Server,由此 DNS 欺骗得以产生并对网络构成威胁。

(3)当 DNS Server 接收到 Domain Name 和 IP Address 相互映射的数据时,就将其保存在本地的 Cache 中。若再有 Client 请求查询此 Domain Name 对应的 IP Address,Domain Server 就会从 Cache 中将映射信息回复给 Client,而无需在 Database 中再次查询。如果黑客将 DNS Request Message 的存在周期设定较长时间,就可进行长期欺骗。

2.2　DNS 欺骗攻击的方式

DNS 欺骗技术常见的有内应攻击和序列号攻击两种。内应攻击即黑客在掌控一台 DNS Server 后,对其 Domain Database 内容进行更改,将虚假 IP Address 指定给特定的 Domain Name,当 Client 请求查询这个特定域名的 IP 时,将得到伪造的 IP。

序列号攻击是指伪装的 DNS Server 在真实的 DNS Server 之前向客户端发送应答数据报文,该报文中含有的序列号 ID 与客户端向真实的 DNS Server 发出请求数据包中含有的 ID 相同,因此客户端会接收该虚假报文,而丢弃晚到的真实报文,这样 DNS ID 序列号欺骗成功。客户机得到的虚假报文中提供的域名的 IP 是攻击者设定的 IP,这个 IP 将把客户带到攻击者指定的站点。

2.3　DNS 序列号欺骗攻击原理

DNS 序列号(ID)欺骗以侦测 ID 和 Port 为基础。在 Switch 构建的网络中,攻击方首先向目标实施 ARP 欺骗。当 Client、攻击者和 DNS Server 同在一个网络时,攻击流程如下:①攻击方向目标反复发送伪造的 ARP Request Message,修改目标机的 ARP 缓存内容,同时依靠 IP 续传使 Data 经过攻击方再流向目的地;攻击方用 Sniffer 软件侦测 DNS 请求包,获取 ID 序列号和 Potr;②攻击方一旦获得 ID 和 Potr,即刻向客户机发送虚假的 DNS Request Message,Client 接收后验证 ID 和 Potr 正确,认为接收了合法的 DNS 应答;而 Client 得到的 IP 可能被转向攻击方诱导的非法站点,从而使 Client 信息安全受到威胁;③Client 再接收 DNS Server 的 Request Message,因落后于虚假的 DNS 响应,故被 Client 丢弃。当 Client 访问攻击者指向的虚假 IP 时,一次 DNS ID 欺骗随即完成。

3　DNS 欺骗检测和防范思路

3.1　检测思路

发生 DNS 欺骗时,Client 最少会接收到两个以上的应答数据报文,报文中都含有相同的 ID 序列号,一个是合法的,另一个是伪装的。据此特点,有以下两种检测办法:

(1)被动监听检测。即监听、检测所有 DNS 的请求和应答报文。通常 DNS Server 对一个请求查询仅仅发送一个应答数据报文(即使一个域名和多个 IP 有映射关系,此时多个关系在一个报文中回答)。因此在限定的时间段内一个请求如果会收到两个或以上的响应数据报文,则被怀疑遭受了 DNS 欺骗。

(2)主动试探检测。即主动发送验证包去检查是否有 DNS 欺骗存在。通常发送验证数据包接收不到应答,然而黑客为了在合法应答包抵达客户机之前就将欺骗信息发送给客户,所以不会对 DNS Server 的 IP 合法性校验,继续实施欺骗。若收到应答包,则说明受到了欺骗攻击。

3.2　防范思路

在侦测到网络中可能有 DNS 欺骗攻击后,防范措施有:①在客户端直接使用 IP Address 访问重要的站点,从而避免 DNS 欺骗;②对 DNS Server 和 Client 的数据流进行加密,Server 端可以使用 SSH 加密协议,Client 端使用 PGP 软件实施数据加密。

对于常见的 ID 序列号欺骗攻击,采用专业软件在网络中进行监听检查,在较短时间内,客户端如果接收到两个以上的应答数据包,则说明可能存在 DNS 欺骗攻击,将后到的合法包发送到 DNS Server 并对 DNS 数据进行修改,这样下次查询申请时就会得到正确结果。

4　DNS 防护方案

4.1　进行 IP 地址和 MAC 地址的绑定

(1)预防 ARP 欺骗攻击。因为 DNS 攻击的欺骗行为要以 ARP 欺骗作为开端,所以如果能有效防范或避免 ARP 欺骗,也就使得 DNS ID 欺骗攻击无从下手。例如可以通过将 Gateway Router 的 Ip Address 和 MAC Address

静态绑定在一起，就可以防范 ARP 攻击欺骗。

(2)DNS 信息绑定。DNS 欺骗攻击是利用变更或者伪装成 DNS Server 的 IP Address，因此也可以使用 MAC Address 和 IP Address 静态绑定来防御 DNS 欺骗的发生。由于每个 Network Card 的 MAC Address 具有唯一性质，所以可以把 DNS Server 的 MAC Address 与其 IP Address 绑定，然后此绑定信息存储在客户机网卡的 Eprom 中。当客户机每次向 DNS Server 发出查询申请后，就会检测 DNS Server 响应的应答数据包中的 MAC Address 是否与 Eprom 存储器中的 MAC Address 相同，要是不同，则很有可能该网络中的 DNS Server 受到 DNS 欺骗攻击。这种方法有一定的不足，因为如果局域网内部的客户主机也保存了 DNS Server 的 MAC Address，仍然可以利用 MAC Address 进行伪装欺骗攻击。

4.2 使用 Digital Password 进行辨别

在不同子网的文件数据传输中，为预防窃取或篡改信息事件的发生，可以使用任务数字签名(TSIG)技术即在主从 Domain Name Server 中使用相同的 Password 和数学模型算法，在数据通信过程中进行辨别和确认。因为有 Password 进行校验的机制，从而使主从 Server 的身份地位极难伪装，加强了 Domain Name 信息传递的安全性。

安全性和可靠性更好的 Domain Name Service 是使用域名系统的安全协议(Domain Name System Security，DNSSEC))，用 Digital Signature 的方式对搜索中的信息源进行分辨，对 DATA 的完整性实施校验，DNSSEC 的规范可参考 RFC2605。因为在设立 Domain 时就会产生 Password，同时要求上层的 Domain Name 也必须进行相关的 Domain Password Signature，显然这种方法很复杂，所以 InterNIC 域名管理截至目前尚未使用。然而就技术层次上讲，DNSSEC 应该是现今最完善的 Domain Name 设立和解析的办法，对防范 Domain Name 欺骗攻击等安全事件是非常有效的。

4.3 优化 DNS SERVER 的相关项目设置

对于 DNS Server 的优化可以使得 DNS 的安全性达到较高的标准，常见的工作有以下几种：①对不同的子网使用物理上分开的 Domain Name Server，从而获得 DNS 功能的冗余；②将外部和内部 Domain Name Server 从物理上分离开并使用 Forwarders 转发器。外部 Domain Name Server 可以进行任何客户机的申请查询，但 Forwarders 则不能，Forwarders 被设置成只能接待内部客户机的申请查询；③采用技术措施限制 DNS 动态更新；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，将访问限制在那些 DNS 功能需要的端口上。

4.4 直接使用 IP 地址访问

对个别信息安全等级要求十分严格的 WEB 站点尽量不要使用 DNS 进行解析。由于 DNS 欺骗攻击中不少是针对窃取客户的私密数据而来的，而多数用户访问的站点并不涉及这些隐私信息，因此当访问具有严格保密信息的站点时，可以直接使用 IP 地址而无需通过 DNS 解析，这样所有的 DNS 欺骗攻击可能造成的危害就可以避免了。除此，应该做好 DNS Server 的安全配置项目和升级 DNS 软件，合理限定 DNS Server 进行响应的 IP 地址区间，关闭 DNS Server 的递归查询项目等。

4.5 对 DNS 数据包进行监测

在 DNS 欺骗攻击中，Client 会接收到至少两个 DNS 的数据响应包，一个是真实的数据包，另一个是攻击数据包。欺骗攻击数据包为了抢在真实应答包之前回复给 Client，它的信息数据结构与真实的数据包相比十分简单，只有应答域，而不包括授权域和附加域。因此，可以通过监测 DNS 响应包，遵循相应的原则和模型算法对这两种响应包进行分辨，从而避免虚假数据包的攻击。

5 结束语

本文对 DNS 解析及 DNS 欺骗的原理进行了阐述，对 DNS 欺骗攻击的方式、检测和防范的思路进行了探讨，最后给出了一些预防 DNS 欺骗的常见方法。相信这些方案的应用，可以大大提高 DNS 的安全性和可靠性。但网络的发展和应用日新月异，在实践中还要不断紧跟技术变化的步伐，不断学习和总结才能有效抵御各种新类型的 DNS 故障。

参考文献：

[1] 滕步炜. DNS 欺骗技术的实现[J]. 连云港职业技术学院学报，2007(12).

[2] 闫伯儒，方滨兴，李斌，等. DNS 欺骗攻击的检测和防范[J]. 计算机工程，2006(21).

[3] 孔政，姜秀柱. DNS 欺骗原理及其防御方案[J]. 计算机工程，2010(2).

[4] 张小妹，赵荣彩. 基于 DNS 的拒绝服务攻击研究与防范[J]. 计算机工程与设计，2008(1).

(责任编辑：杜能钢)