第 36 卷 第 3 期 计 算 机 工 程 2010 年 2 月
Vol.36 No.3 Computer Engineering February 2010
·安全技术· 文章编号：1000—3428(2010)03—0125—03 文献标识码：A 中图分类号：TP393.08

DNS 欺骗原理及其防御方案

孔 政，姜秀柱
(中国矿业大学计算机科学与技术学院，徐州 221008)

摘 要：针对 DNS 欺骗表现出的危害性大、隐蔽性强的特点，通过对 DNS ID 欺骗攻击及 DNS 缓存中毒攻击的原理进行剖析，应用概率学理论证明了“生日攻击”的危害，分别给出相应的防御方案。对于不同类型的用户可以根据自身的条件和对信息安全要求级别的高低，采用适合自己的应对方案。

关键词：DNS 欺骗；ARP 欺骗；DNS ID 欺骗；DNS 缓存中毒；生日攻击

DNS Spoofing Principle and Its Defense Scheme

KONG Zheng, JIANG Xiu-zhu
(School of Computer Science and Technology, China University of Mining and Technology, Xuzhou 221008)

【Abstract】DNS spoofing presents the characteristics of severe harm and high dormancy. By analyzing the principle of DNS ID spoofing attack and DNS cache poisoning attack, this paper proves the harm of “birthday attack” by using the probability theory, and puts forward some corresponding defense methods. In conclusion, to different kinds of users, they can use practical and effective defense measures according to their conditions and demand levels of information security.

【Key words】 DNS spoofing; ARP spoofing; DNS ID spoofing; DNS cache poisoning; birthday attack

1 概述

域名系统(Domain Name System, DNS)是一个可以将域名和 IP 地址相互映射的分布式数据库。由于它是互联网的核心服务之一，在其中扮演着极为重要的角色，其安全与否对整个互联网的安全性有着重要的影响。因为在 DNS 协议设计之初，设计者并未过多地考虑安全问题，导致 DNS 本身留有很多安全隐患。特别是在 2008 年，有关 DNS 的严重漏洞(US-CERT VU#800113[1]; CVE-2008-1447)又被发现，其安全性又一次引起了人们的重视和忧虑。

目前，针对 DNS 协议存在的问题，很多专家给出了解决办法。IETF 提出的域名系统的安全协议(Domain Name System Security, DNSSEC)[2]旨在解决 DNS 的安全问题，但由于需要占用更多的系统开销和网络资源，还要对相应的数据库和系统管理软件进行升级，并且新的软件尚处于测试阶段，离 DNSSEC 普及性地应用还有一定的距离。现在，主要的应对办法是升级 DNS 软件和加强服务器的安全配置，除此之外，尚未发现较有效的防范措施[3]。

以侦听为基础的 DNS 欺骗(DNS spoofing)和 DNS 缓存中毒(DNS cache poisoning)对目标主机都具有欺骗性质，本文把这 2 种攻击方式都列入 DNS 欺骗攻击并加以讨论。为了予以区分，把前者称之为 DNS ID 欺骗(DNS ID spoofing)，并且尝试分别给出 2 类攻击的应对方案。针对 DNS 协议的攻击还有很多，诸如“洪水”攻击和服务器攻陷等其他攻击手段不在本文研究范围之内。

2 DNS 服务原理

DNS 服务的工作原理如图 1 所示。如果某用户需要对域名 www.example.com 进行解析，以得到其相应的 IP 地址；而且假定本地 DNS 服务器不是目标域名授权 DNS 服务器和其缓存中没有相应的记录。

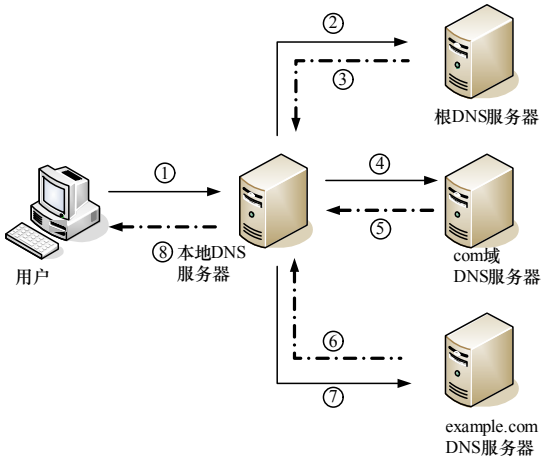

图 1 DNS 服务原理示意图

其查询过程如下：

①~②：用户向本地 DNS 服务器发出 DNS 请求，询问 www.example.com 的地址；本地 DNS 服务器发现没有相应记录，转而向根目录发出查询包。

③~⑦：根 DNS 服务器接到请求，并将 com 域服务器的地址返回给本地 DNS 服务器；后者继续向 com 域服务器发出请求，com 域服务器返回 example.com 授权域名服务器的地址；而后再次发出请求，并得到 www.example.com 的地址。

⑧：本地 DNS 服务器得到地址后，以 DNS 应答包的方

作者简介：孔 政(1981－)，男，硕士研究生，主研方向：计算机网络安全；姜秀柱，副教授
收稿日期：2009-09-30 **E-mail**：konglzheng@yahoo.com.cn

式传给用户，如果其具有缓存机制的话，还需更新自己的缓存记录。在客户机收到 DNS 服务器给它发过来的 DNS 应答之后，会去查询收到的数据包中的 ID(Query ID，或者 Transaction ID，以下都简称为 ID)和端口号是否和自己发出去的一致，如果一样则接受为正确的回答；不一样以及再次接受到同一域名的应答包都抛弃。至此 DNS 服务结束。由于这一确认机制过于简单，因此使之成为被攻击者利用的漏洞。

3 DNS ID 欺骗攻击及其防御方案

3.1 DNS ID 欺骗攻击原理

DNS ID 欺骗以监听 ID 和端口号为基础，如果是在交换机搭建的网络环境下，欺骗者首先要向攻击目标实施 ARP 欺骗。图 2 是一个 DNS ID 欺骗(DNS ID spoofing)的实例。假设用户、欺骗者和 DNS 服务器同在一个局域网内。

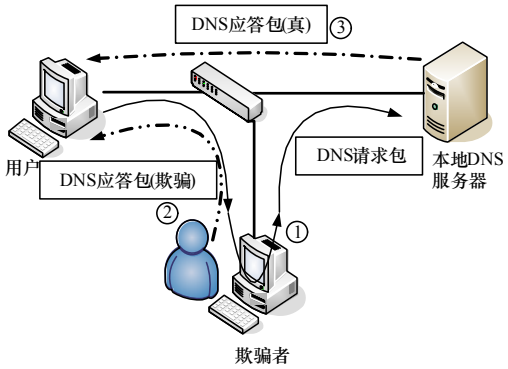

图 2 网内 DNS spoofing 攻击示意图

攻击流程如下：

①：欺骗者通过向攻击目标以一定的频率发送伪造 ARP 应答包改写目标机的 ARP cache 中的内容，并通过 IP 续传使数据流过欺骗者的主机再流向目的地；欺骗者配合 Sniffer 软件监听 DNS 请求包，取得 ID 和端口号。

②：欺骗者取得 ID 和端口号后，立即向攻击目标发送相应的伪造 DNS 应答包，用户收到后确认 ID 和端口号无误，以为收到正确的 DNS 应答包；而其实际的地址很可能被导向攻击者想让用户访问的恶意网站，用户的信息安全受到威胁。

③：用户再次收到 DNS 服务器发来的 DNS 应答包，由于晚于伪造的 DNS 应答包，因此被用户抛弃；用户的访问被导向攻击者设计的地址，一次完整的 DNS ID 欺骗完成。

3.2 防御方法

根据此种攻击的特点，有以下的应对方案可以考虑：

(1)对少数信息安全级别要求高的网站避免使用 DNS。因为 DNS 欺骗中相当一部分的目的是窃取用户的私密信息，而对于大部分用户而言，其访问网站中的大多数都不涉及此类信息，所以在访问涉及个人私密信息的网站时(比如通过网上银行进行交易)，可以直接通过 IP 地址访问，这样就可以绕开 DNS 服务，DNS 欺骗自然无从谈起，其危害性就大大降低了。因为涉及敏感信息的网站只占很少的一部分，对于绝大多数用户而言，这种方法几乎不会对其使用产生什么影响；又由于大部分用户受自身条件所限，不足以对所处的网络环境产生什么影响，并且对信息安全要求不是太高，因此该方法不失为一种简单有效的方法，而且对于所有涉及 DNS 的攻击均有效。

(2)防范 ARP 攻击。因为此类攻击需要以 ARP 欺骗为基础，所以较为直接的方法是谨防受到 ARP 欺骗攻击。避免了 ARP 攻击的可能，自然就无法进行 DNS ID 欺骗。

4 DNS 缓存中毒攻击及其防御方案

4.1 DNS 缓存中毒原理

在不得到 ID 和端口号的情况下不可能完成 DNS 欺骗攻击。原理是，如果在已知端口号的前提下，通过发送大量的 DNS 应答包来猜测攻击目标的 DNS 请求包的 ID 号，如果所发送的伪造应答包中存在和请求包的 ID 一致的情况，也就是产生了所谓的“碰撞”，则欺骗成功。16 位的 ID 号取值范围为 0~65 535，共有 65 536 种可能性，想要使其攻击的成功率可以达到 50%，至少需要发送 32 768 个完全不同 ID 号的应答包。如果不知道端口号，ID 和端口号的组合空间比原来扩大了 6 万多倍，相应的攻击成功率也就极大地降低了。不幸的是，有很多的 DNS 服务器的端口都是固定的，只需要一个 DNS 请求，就可以从反馈当中得知端口号。这样的结果使得 DNS 缓存中毒攻击成为可能。可是要得到 50%的成功率，在短时间内发送 32 768 个包，还要赶在真正的应答包到来之前发生“碰撞”，其操作难度较大。如果很好地利用“生日攻击”就可以只发送较少的数据包，同样能达到欺骗的效果。

“生日攻击”的攻击目标必须是 DNS 服务器，其涉及到一个叫作“生日悖论”的数学模型。“生日悖论”是指 23 个人中有人生日是同一天的可能性大于 50%。通过概率论的知识，可知 2 个人的生日是同一天的可能性是：P(2)=1-1×(364/365)；3 个人中有生日相同的概率是：P(3)=1-1×(364/365)×(363/365)；以此类推，P(4)=1-1×(364/365)×(363/365)×(362/365)；…；P(n)=1-1×(364/365)×…(365-(n-1))/365，(n=1,2,…,365)；可得出 P(23)>50%，即 23 人中有可能其中有人的生日是相同的。从中可以看出，一个有 365 个元素的空间，只需 23 个元素其间产生“碰撞”的概率就高于 50%。

如果对一台本地 DNS 服务器发动“生日攻击”，如图 3 所示[4]，而且假定本地 DNS 服务器不是目标域名的授权 DNS 服务器和其缓存中没有相应的记录。

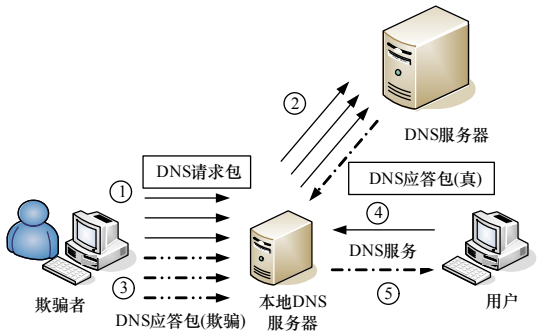

图 3 DNS cache poisoning“生日攻击”示意图

攻击流程如下：

①~②：欺骗者向目标服务器发送数量为 q 的 DNS 请求包，如果在没有做特殊配置的情况下，服务器会转而向上级服务器发送同样数量的查询包。这一漏洞(US-CERT VU#457875)成为了发动“生日攻击”的有利条件，它对相同的请求包生成大量的查询包，使得“生日攻击”变得简单了许多。

③：欺骗者再向攻击目标发送数量为 r 的伪造应答包，如果产生了 ID 号的“碰撞”，则服务器被欺骗收到了 DNS 应答包，如果其具有缓存机制，并把记录写入自己的 Cache，那么针对 DNS 服务器的“生日攻击”宣告成功。

④~⑤：在此条记录的缓存生存周期内，凡是以这台服务器为 DNS 服务器的客户机访问同样域名的网站都会被导向

错误的地址。

为了研究攻击者究竟需要发送多少个请求和应答包，才能组织一次有效的攻击，在端口号固定而 ID 号随机的情况下，假设欺骗者先发送了 q 个请求包，再发送 r 个应答包，并保证 r 个应答包中 ID 号各不相同，则第 1 个应答包到达目标机，发送“碰撞”的可能性为

$$p(1)=\frac{q}{35\,536}$$

第 2 个包“碰撞”的可能性为

$$p(2)=\frac{q}{35\,536-1}$$

以此类推，第 n 个包到达，发送“碰撞”的可能性为

$$p(n)=\frac{q}{35\,536-(n-1)}$$

则第 n 个包到达，不发送“碰撞”的可能性为

$$Q(n)=1-p(n)=1-\frac{q}{35\,536-(n-1)}$$

所以，在发送 q 个请求包的前提下，发送 r 个 ID 各不相同的应答包，最后得出 DNS 请求包和应答包发生“碰撞”的概率为[5]

$$P(r)=1-\prod_{n=1}^{r}Q(n),\ Q(n)=1-\frac{q}{35\,536-(n-1)},\ n=1,2,\cdots,r \quad (1)$$

根据式(1)可以得知，在理想状态下所发送的数据包数和“碰撞”成功率的对应关系如表 1 所示。根据实验可知，当 $r+q$ 为定值时，令 $q=r$，也就是攻击者发送请求包和应答包的数量相等，“碰撞”成功率最大。表 1 中的数据包数为分别发送请求包/应答包的数量。

表 1　数据包数量和“碰撞”成功率对应关系

数据包数	生日攻击成功率/(%)	传统攻击成功率/(%)
100	14.17	0.15
200	45.79	0.31
213	50.07	0.33
300	74.83	0.46
400	91.43	0.61
450	95.55	0.69
500	97.86	0.76

从表 1 和图 4 中的数据可以得知，如果采用“生日攻击”，只需要发送很少的数据包，就可以达到很好的效果。随着数据包数量的增加，相对于传统 DNS 欺骗攻击，“生日攻击”的优势明显。当然，这个概率只是理论上的，并不是攻击成功的概率，攻击者要想成功地使目标机的 Cache 中毒还需要其他一些因素共同决定，比如：这些伪造的应答包要赶在真的应答包到来之前发送至目标主机。有些攻击者会提前向上层 DNS 服务器发送大量的查询包，以延缓对真正请求的响应，从而为成功地攻击目标赢得足够的时间。还和不同的 DNS 软件及其设置相关，比如：有些软件会对相同的请求包数量进行限制，这样会增加攻击的难度。即便如此，“生日攻击”的危害仍然不能忽视。可以使 DNS 服务器 Cache 中毒的方法还有许多，限于本文的篇幅，不再赘述。

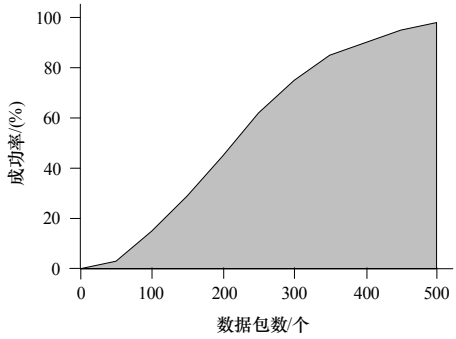

图 4　数据包数量和“碰撞”成功率的对应关系

4.2　防御方案

除上文所涉及到的 2 种防范措施外，根据“生日攻击”的特点，有下面的应对方案可以考虑：

(1)采用随机端口。如果作为被攻击的服务器在发送 DNS 请求时使用随机端口，这样可以使 ID 号和端口号的组合空间扩大 6 万多倍，大大增加攻击的难度。

(2)为信息安全要求高的网站建立标准 IP 映射表。作为 DNS 服务器，有能力为少部分网站(比如涉及私密信息的网站或经常访问的网站)制作静态的标准 DNS 映射表，这样可以保证这种攻击对这部分网站无从下手。

(3)被动检测法。由于此类攻击往往需要在短时间内发送大量的针对同一个域名的请求包，这显然并不合乎常理，因此可以针对这一特点进行 DNS 欺骗检测，或者限制发送查询包的数量，其效率较高。

5　结束语

本文针对 2 种主要的 DNS 欺骗攻击的原理，给出了多种防范措施，并认为不同的用户可以根据自身的条件和对信息安全要求级别的高低，采用适合自己的应对方案。虽然从理论上要做到百分之百地抵御 DNS 欺骗难度很高，但是仍然可以通过上述防范措施大大地降低 DNS 欺骗攻击成功的概率。在 DNS 欺骗攻击中，还有一类较为特殊和复杂的相空间分析欺骗攻击，这将是下一步工作的重点。

参考文献

[1] US-CERT. Multiple DNS Implementations Vulnerable to Cache Poisoning[EB/OL]. (2008-07-08). http://www.kb.cert.org/vuls/id/800113.

[2] Eastlake D. Domain Name System Security Extensions[S]. RFC 2535, 1999.

[3] 闫伯信, 方淇兴, 李　斌, 等. DNS 欺骗攻击的检测和防范[J]. 计算机工程, 2006, 32(21): 130-135.

[4] Stewart J. DNS Cache Poisoning——The Next Generation[EB/OL]. (2003-01-27). http://www.secureworks.com/research/articles/cache poisoning.

[5] US-CERT. Various DNS Service Implementations Generate Multiple Simultaneous Queries for the Same Resource Record[EB/OL]. (2002-11-19). http://www.kb.cert.org/vuls/id/457875.

编辑　顾逸斐