第32卷 第21期 计 算 机 工 程 2006年11月
Vol.32 No.21 Computer Engineering November 2006
·安全技术· 文章编号：1000—3428(2006)21—0130—03 文献标识码：A 中图分类号：TP393.08

DNS欺骗攻击的检测和防范

闫伯儒，方滨兴，李 斌，王 垚
(哈尔滨工业大学国家计算机信息内容安全重点实验室，哈尔滨 150001)

摘 要：DNS是目前大部分网络应用的基础，对它的攻击将影响整个Internet的正常运转。DNS欺骗攻击是攻击者常用的手法，它具有隐蔽性强、打击面广、攻击效果明显的特点，但是目前对这种攻击还没有好的防范策略。在分析DNS欺骗原理的基础上提出了3种攻击检测手段和3种识别攻击包的方法，对于提高DNS的安全性和抗攻击性具有积极的作用。

关键词：DNS；DNS欺骗；攻击检测

Detection and Defence of DNS Spoofing Attack

YAN Boru, FANG Binxing, LI Bin, WANG Yao
(National Key Lab on Computer Context Information Security, Harbin Institute of Technelogy, Harbin 150001)

【Abstract】DNS is a critical component of the operation of Internet applications. The Internet is greatly affected if DNS is attacked. DNS spoofing is one of the most popular attack means with the character of high dormancy and good attack effection. But so far, little is done to defend the systerm against this attack. Three methods are presented to detect DNS spoofing attack, and then another three techniques are proposed to identify the bogus packets and the right ones to ensure DNS service even attacked.

【Key words】Domain name system (DNS); DNS spoofing; Attack detection

DNS是一个用于管理主机名字和地址信息映射的分布式数据库系统，它将便于记忆和理解的名称同枯燥的IP地址联系起来，大大方便了人们的使用。DNS是大部分网络应用的基础，但是由于协议本身的设计缺陷[1]，没有提供适当的信息保护和认证机制，使得DNS很容易受到攻击。2005年3月美国系统网络安全协会的互联网海量数据中心（ISC）发出了关于DNS欺骗攻击的警告，新一轮攻击中大批.COM成为牺牲品，至少有1 300个域名被诱骗到被破坏的服务器。而在计算机安全组织美国系统网络安全协会(SANS Institute)公布的2004年前20位网络安全隐患排行榜中，BIND域名系统更是排在Unix及Linux相关安全隐患的首位[2]。由此可见防范对DNS的攻击，确保DNS系统的安全已经到了刻不容缓的地步。

一直以来，很多学者都在探讨DNS安全性的问题，对于DNS协议所固有的安全缺陷，给出了一些解决方案。IETF的域名系统安全工作组提出了域名系统安全扩展协议DNSSEC，该协议增加了认证机制，增强了协议本身的安全性。但是目前该协议在系统效率、密钥管理等方面还存在一定的问题，而且离大规模的普及和应用还有一定的距离。因此除了对DNS协议本身的安全研究之外，也有很多文章探讨了在现有的基础上的一些安全方案，主要是升级服务器软件，对DNS系统严格配置，禁止相关的功能等被动消极的防范手段[3]。对一些难以避免的攻击如DNS欺骗攻击缺乏必要的解决方案。

1 DNS欺骗攻击原理

DNS作为Internet的基础服务，受到来自各方面的威胁，对于DNS的攻击主要有以下几种（如表1所示），从比较的情况来看，它们各具特色。

从表1可以看出，DNS欺骗和缓存中毒攻击都是利用了欺骗的手段，而且都比较容易实施，因此这两种攻击危害也最大。另外DNS欺骗主要利用协议本身的认证缺陷，难以防范。而缓存中毒则更多地依赖于DNS服务器软件自身的漏洞，只要升级软件的最新版本并严格进行配置，对这种攻击的防范能力将明显提高。

表1 DNS攻击比较

DNS攻击类型	主动性	攻击流量	被攻击者	攻击手段	攻击难度
DNS欺骗 (DNS Spoofing)	被动	小	客户端/服务器	欺骗	最容易
缓存中毒 (Cache Poisoning)	主动	大	服务器	欺骗	较容易
服务器攻陷 (Server Compromising)	主动	小	服务器	漏洞入侵	最难
拒绝服务 (Denial of Service)	主动	最大	服务器	耗费资源	较难

有些学者也把缓存中毒攻击称为DNS欺骗攻击[4]。为明确区分这两种攻击，本文中所指DNS欺骗攻击将不包括缓存中毒攻击，缓存中毒也不作为本文讨论的重点。

1.1 DNS解析原理

在分析DNS欺骗攻击原理之前，先界定一下DNS的工作原理。假设要查询的域名为www.hit.edu.cn，并假设客户端和首选DNS服务器满足以下条件。

(1) 首选DNS服务器和客户机首次启动，并且没有本地缓存信息。

(2) 首选DNS服务器不是目标域名的授权域名服务器。

作者简介：闫伯儒((1982－)，男，硕士，主研方向：DNS测量和安全加固；方滨兴，教授、博导；李 斌，教授；王 垚，博士

收稿日期：2006-01-10 **E-mail：**yanboru@pact518.hit.edu.cn

具体查询的过程如图 1 所示，步骤如下：

(1) 客户端首先向首选 DNS 服务器递归查询 www.hit.edu.cn。

(2)首选 DNS 服务器检查本地资源记录，若存在则作授权回答；若不存在，则检查本地缓存，如存在则直接返回结果。若本地资源记录和缓存中都不存在时，则向根服务器迭代查询。

(3)根服务器返回 CN 域的授权域名服务器的地址，首选 DNS 服务器继续向 CN 授权服务器迭代查询。

(4)CN 域权威服务器返回 edu.cn 域的授权域名服务器地址，首选 DNS 服务器如此迭代查询，直到得到对于域名 www.hit.edu.cn 的授权回答，保存在本地缓存中，并返回给客户端，完成此次查询。

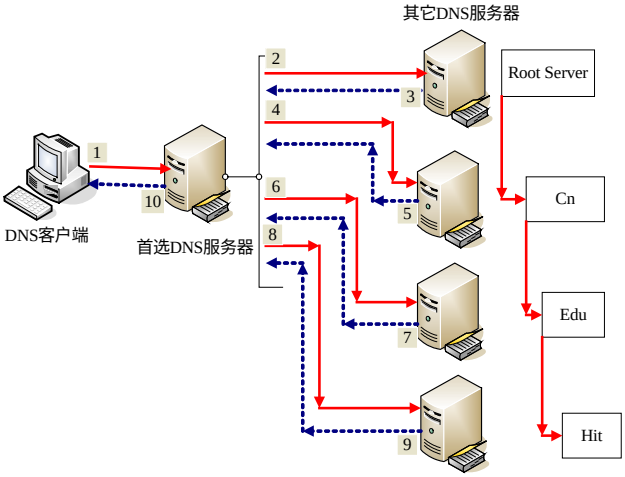

图 1 域名解析过程

1.2 DNS 欺骗攻击原理

由于 DNS 协议在设计上的缺陷，在 DNS 报文中只使用一个序列号来进行有效性鉴别，并未提供其它的认证和保护手段，这使得攻击者可以很容易地监听到查询请求，并伪造 DNS 应答包给 DNS 客户端，从而进行 DNS 欺骗攻击。

目前所有 DNS 客户端处理 DNS 应答包的方法都是简单地信任首先到达的数据包，丢弃所有后到达的，而不会对数据包的合法性作任何的分析。这样，只要能保证欺骗包先于合法包到达就可以达到欺骗的目的，而通常这是非常容易实现的。DNS 欺骗攻击可能存在于客户端和 DNS 服务器间，也可能存在于各 DNS 服务器之间，但其工作原理是一致的，如图 2 所示。

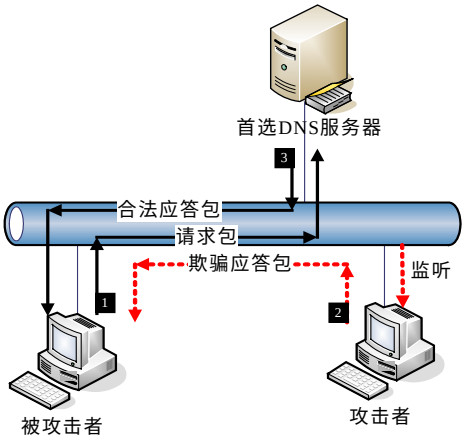

图 2 DNS 欺骗攻击

仍以 www.hit.edu.cn 为例，假设伪造 IP 为 1.2.3.4，具体的欺骗过程如下：

(1)DNS 客户端向首选 DNS 服务器发送对于 www.hit.edu.cn 的递归解析请求。

(2)攻击者监听到请求，并根据请求 ID 向请求者发送虚假应答包，通知与 www.hit.edu.cn 对应的 IP 地址为 1.2.3.4。

(3)本地 DNS 服务器返回正确应答，但由于在时间上晚于监听者的应答，结果被丢弃。

(4)攻击完成，客户端对 www.hit.edu.cn 的访问被重定向到 1.2.3.4。

2 DNS 欺骗攻击的检测

根据 1.2 节讨论，如果受到欺骗攻击，那么客户端应该至少收到两个应答包，一个合法应答包，一个欺骗攻击包。根据这个特点就可以通过一定的方法检测这种攻击。根据检测手段的不同，将其分为被动监听检测、虚假报文探测和交叉检查查询 3 种：

(1)被动监听检测：该检测手段是通过旁路监听的方式，捕获所有 DNS 请求和应答数据包，并为其建立一个请求应答映射表。如果在一定的时间间隔内，一个请求对应两个或两个以上结果不同的应答包，则怀疑受到了 DNS 欺骗攻击，因为 DNS 服务器不会给出多个结果不同的应答包，即使目标域名对应多个 IP 地址，DNS 服务器也会在一个 DNS 应答包中返回，只是有多个应答域(Answer Section)而已。

(2)虚假报文探测：该检测手段采用主动发送探测包的手段来检测网络内是否存在 DNS 欺骗攻击者。这种探测手段基于一个简单的假设：攻击者为了尽快地发出欺骗包，不会对域名服务器 IP 的有效性进行验证。这样如果向一个非 DNS 服务器发送请求包，正常来说不会收到任何应答，但是由于攻击者不会验证目标 IP 是否是合法 DNS 服务器，他会继续实施欺骗攻击，因此如果收到了应答包，则说明受到了攻击。

(3)交叉检查查询：所谓交叉检查即在客户端收到 DNS 应答包之后，向 DNS 服务器反向查询应答包中返回的 IP 地址所对应的 DNS 名字，如果二者一致说明没有受到攻击，否则说明被欺骗。

以上讨论了 3 种 DNS 欺骗攻击的检测手段，其中被动监听检测法属于被动方式，其它两种属于主动方式。被动监听检测法不会造成网络的附加流量，但它是一种消极的应对方式，无法检测潜在的攻击。虚假报文探测法需要主动发送大量探测包，会增加网络负担。另外 DNS 欺骗攻击一般只欺骗特定的域名，这样探测包中待解析域名的选择就有很大的不确定性，从而增加了探测的难度。而交叉检查查询位于二者之间，在被动检测的基础上，对收到的应答包进行主动验证，但是这种方法更多地依赖于 DNS 服务器的反向查询服务，大量的 DNS 服务器并没有提供这种服务。

3 种检测手段各有优缺点，在实际应用中可以将三者有效地结合起来，取长补短，从而达到好的检测效果。

3 DNS 欺骗攻击的防范

通过对合法应答包和欺骗应答包的分析发现，欺骗应答包一般来说比较简单，通常只有一个应答域，没有授权域和附加域。这也正符合欺骗攻击者要尽快将欺骗数据包返回给客户端的初衷，因为只有尽可能地节约数据包构造的时间才能使欺骗包早于合法包到达。而合法应答包的信息则比较丰富，除了可能有多个应答域之外，通常还带有授权域，附加

记录域等。如果根据一定的规则，能够区分开欺骗包和合法包，那么就可以躲避 DNS 欺骗攻击，从而使系统具有抗攻击能力。以下是几种可行的防范措施：

(1)加权法。这种方法首先要根据统计分析，给 DNS 应答包中的各个字段一个相应的可信度阈值，然后根据数据包情况计算最终可信度，最后选择可信度最高的应答包。权值为有符号数，正表示加上相应的值，负则减去。计算规则描述如下：

设数据包可信度权值为 S，W_i 为第 i 个属性的权值，N_i 表示第 i 个属性的个数，m 为总的属性数，则有如下公式：

$$S = \sum_{i=1}^{m} W_i * N_i$$

这种方法的准确性在很大程度上依赖于权值分布，只要权值设置得合理，就可以达到满意的识别效果。

(2)贝叶斯分类法。这种方法利用模式分类的思想，设计一个两类贝叶斯分类器来区分合法和欺骗包。首先根据统计信息抽取合法包和欺骗包的特征，然后统计这些特征的概率分布，并由此设计一个简单的两类贝叶斯分类器，来指导欺骗包和合法包的识别。本文只是提出识别的思想，分类器的设计不是本文讨论的重点，此处仅以一个特征为例做简单的介绍。

根据国内外统计数据，发现同一域名的 DNS 服务器的分布和个数具有一定的特征。Men&Mice[5]分别对 GOV、COM 域以及国家顶级域的 DNS 服务器的分布做了调查，结果如表 2 所示。

表 2 域名服务器分布统计

测试日期	所属域	所有服务器位于同一子网(%)	单授权域名服务器(%)
2001-11-08	GOV	23.15%	13.07%
2001-11-30	COM	36.2%	6.8%
2001-10-03	DK	55.2%	8.8%
2001-10-03	FI	48.2%	2.3%
2001-10-03	NO	29.5%	5.7%
2001-10-03	SE	41.1%	4.0%

作者对国内 Top100 网站的调查也显示出类似结果，如图 3 所示。

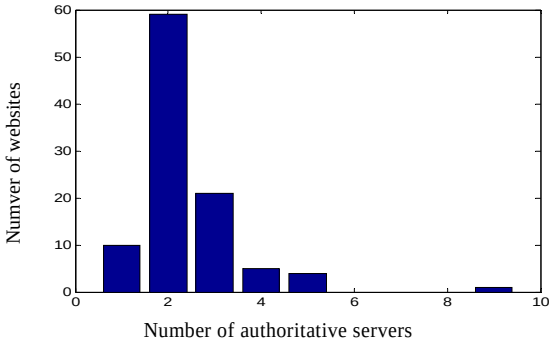

图 3 国内 Top100 网站域名服务器分布

从以上统计可以看出，超过 90%的域名具有多个授权域名服务器，也就是说一个合法 DNS 应答包中包含多个授权域的概率为 90%。可以将此项作为设计贝叶斯分类器的关键特征。

设 W_1 表示数据包为合法包，W_2 表示数据包为欺骗包，特征 x 表示数据包中包含授权域的个数，n 为一段时间内同一个 DNS 请求收到的结果不同的应答数，由贝叶斯公式：

$$P(W_1|x)=\frac{P(W_1)p(x|W_1)}{P(x)}, P(W_2|x)\frac{P(W_2)p(x|W_2)}{P(x)}$$

且 $P(W_1|x)+P(W_2|x)=1$

其中：

$P(W_1)$:数据包为合法包的概率，因为只有一个合法包，所以取值为 1/n；

$P(W_2)$:数据包为欺骗包的概率，取值为 1-$P(W_1)$=1-1/n；

$P(W_1|x)$:当数据包中包含 x 个授权域时，数据包为合法包的概率；

$P(W_2|x)$:当数据包中包含 x 个授权域时，数据包为欺骗包的概率；

$p(x|W_1)$:合法 DNS 应答包中授权域个数的分布，如图 3。

$p(x|W_2)$:欺骗 DNS 应答包中授权域个数的分布，分布函数为

$$P(x|W_2)=\begin{cases}0.1, x>=1\\ 0.9, x=0\end{cases}$$

$$P(x)=P(x|W_1)P(W_1)+P(x|W_2)P(W_2)$$

构造两类分类器：

$$g(x)$$
$$=P(W_1|x)-P(W_2|x)$$
$$=\frac{P(W_1)P(x|W_1)-P(W2)P(x|W_2)}{P(x)}$$

由于归一化常数 P(x)对最终分类没有影响，因此可将其去掉，得

$$g'(x)$$
$$=P(W_1)P(x|W_1)-P(W_2)P(X|W_2)$$
$$=\frac{1}{n}*P(x|W_1)-\frac{n-1}{n}*P(x|W_2)$$
$$=\frac{P(x|W_1)-\frac{1}{n}*P(x|W_2)}{n}$$

设此贝叶斯分类器的误差率为 P(error|x)，可以得出以下结论：

$$P(error|x)=\begin{cases}P(W_1|x), P(W_1|x)<=P(W_2|x)\\ P(W_2|x), P(W_1|x)>P(W_2|x)\end{cases}$$

即

$$P(error|x)=\min\left[P(W_1|x), P(W_2|x)\right]$$

这样就可以通过此分类器来判断合法应答包了。给定一个数据包，首先统计出其授权域个数，然后计算 g’(x)，如果 g’(x)>0 则为合法包，否则为欺骗包，其中误差为 P(error|x)。当然，单独采用一个特征可能带来较高的误差率，本文只是提出一种思想，具体的分类器设计和误差分析见参考文献[6]。

(3)交叉验证法。这种方法在 DNS 欺骗的检验中介绍过了，是由客户端收到 DNS 应答包之后，向 DNS 服务器反向查询应答包中返回的 IP 地址所对应的 DNS 名字来进行判断。

以上讨论了 3 种识别欺骗应答包和合法应答包的方法，其中加权法和贝叶斯分类法有类似之处，都要基于统计数据的分析。加权法依赖于权值策略的制定，贝叶斯分类法依赖于数据包关键特征的提取和其概率分布的统计。交叉验证法则可以和欺骗检验同时完成，但是对反向解析服务依赖较大，难以大范围使用。以上 3 种识别方案可以结合起来用，相辅相成，优势互补，从而达到好的识别效果。

4 实验结果与分析

实验采用著名的 ADMID 作为 DNS 攻击工具，但是由于

（下转第 135 页）

在 RAS/H.225.0 信令消息内，按上述方法设置数据结构，并完成相应签名运算后，发送给接收实体。签名消息依赖于终端与网络安全策略，决定是对整个信令消息还是仅仅为其中一部分。

接收实体收到该信令消息后，立刻检验发给它的那些 tokenOID 所指示的签名，完成下列安全认证过程：

(1)通过验证时间戳的生存期和 random 值的唯一性来抵御 DoS 攻击；

(2)通过对 generalID 身份与自己的识符比较，验证发送者是否为合法用户；

(3)验证 SendersID 是否与证书内一致及是否具有相应的访问权限；

(4)消息签名是否与自身验证计算的签名相匹配，以验证消息是否被中途篡改；

(5)通过对接收到的证书的检验，验证发送实体是否为合法注册实体及电子商务中的不可否认性。

验证了发送实体合法性后，可利用 dhkey 中指明的 Diffie-Hellman 密钥协商算法，在返回的响应消息(GCF,RCF)中，完成会话密钥的协商与交换。

4.2 安全呼叫信令信道(H.225.0)与媒体信道的建立

完成终端安全接入网络后，可通过 ARQ/ACF 或 LRQ/LCF 信令交互，基于网络接入过程中所安全交换的会话密钥，利用对称密码技术实现安全认证/完整性并建立起安全信道；利用 Diffie-Hellman 算法可为多媒体终端之间的通信协商出连接及媒体流加密的会话密钥。利用实时传输协议/实时传输控制协议[6] (RTP/RTCP) 实现基于分组的媒体通信的机密性。

5 结论

本文通过对 H.235 协议框架内的认证、隐私及完整性的研究，提出一种基于椭圆曲线密码技术，对 H.323 系统实施增强安全保护。针对通用处理器的特点，设计与实现了具有可伸缩结构、实时有效 ECC 快速算法，使得由该算法实现的 ECC 软件引擎既可用于受限处理器平台，如简单智能电话终端，也能用于高端服务器上，如网守。所设计的点乘与点加算法，相对于 IEEE P1363 标准中给出的算法[8]，速度可提高 10%~15%。最后，基于所给出的 ECC 安全方案，结合 H.323 终端的通信流程，完整实现了增强 IP 分组多媒体通信安全与保密。

参考文献

1 ITU-T. H.323-2003 Packet-based Multimedia Communications Systems[S]. 2003.

2 ITU-T. H.245-2003 Control Protocol for Multimedia Communication[S]. 2003.

3 ITU-T. H.225.0-2003 Call Signalling Protocols and Media Stream Packetization for Packet-based Multimedia Communication Systems[S]. 2003

4 ITU-T. H.235-2000 Security and Encryption for H-series (H.323 and Other H.245-based) Multimedia Terminals[S]. 2000.

5 ITU-T. X.509 | ISO/IEC 9594-8-2001 Information Technology – Open Systems Interconnection–The Directory: Authentication Framework [S]. 2001.

6 RTP Payload for Redundant Audio Data[S]. IETF RFC 2198, 1997.

7 National Institute for Standards and Technology. FIPS 186-1993 Digital Signature Standard[S]. http://csrc.ncsl.nist.gov/fips/, 1993.

8 IEEE P1363. Standard for Public-key Cryptography: Work Draft [EB/OL]. http://www.secg.rog/, 2001.

9 卢　忱. 基于椭圆曲线方法的医学信息安全与保密研究[D]. 西安: 西安交通大学, 2004.

（上接第 132 页）

ADMID 本身没有对授权域和附加域进行处理，因此还不能完全代表所有的攻击模式。为此作者在欺骗包的构造中引入了 10%的授权域浮动因子，使得欺骗包的授权域以 10%的概率浮动，从而增加实验的真实性。本实验分别采用加权法和贝叶斯分类法对国内 Top100 网站进行了域名解析测试，实验结果如表 3 所示。

表 3 域名欺骗攻击识别实验结果

识别方案	DNS 请求次数	欺骗次数	攻击检测成功次数	合法包识别成功次数
加权法(1,0,0)	1 000	1 000	973	726
加权法(1,1,1)	1 000	1 000	984	973
贝叶斯分类(单特征)	1 000	1 000	977	936

表 3 加权法括号内为权值分配策略，其依次为应答域、授权域和附加域的权值。从表 3 中可以看出，当采用加权法时，仅通过应答域来判断时，识别率为 72.6%，误差较大；而当调整权值策略，综合考虑应答域、授权域、附加域时，识别率就大大提高，平均达到了 97.3%。由于目前的攻击工具构造的虚假报文都比较简单，因此单特征的贝叶斯分类法的识别率也比较高，达到了 93.6%。当然如果攻击工具调整了报文信息，权值分布和特征都要作相应的调整才能达到满意的识别效果。

5 总结

网络攻防一直是推动网络安全向前发展的源动力。只有不断地发现网络的安全弱点并不断改正，才能使整个网络更加健康和完善。本文基于当前的 DNS 架构，提出了对于 DNS 欺骗攻击的全新的检测和防范方案，对于提高 DNS 的安全性和抗攻击性具有积极的作用。缓存中毒攻击是针对 DNS 的另一攻击手段，对它的检测和防范，以及对攻击者的反向追踪将是我们下一步工作的重点。

参考文献

1 Mockapetris P. Domain Names-Concepts and Facilities[S]. RFC1034, 1987.

2 SANS Institute. The Twenty Most Critical Internet Security Vulnerabilities[Z]. http://www.sans.org/top20/, 2004.

3 林曼筠. 域名服务器的安全保护[J]. 网络安全技术与应用, 2001, (1): 21-24.

4 Lioy A, Maino F, Marian M. DNS Security[C]. Proc. of Terena Networking Conference, 2000.

5 Men & Mice. Single Point of Failure Research[Z]. http://www.menandmice.com/6000/6300_single_point_failure.html, 2001.

6 Duda R O, Hart P E, Stork D G. Pattern Classification (2nd Edition) [M]. New York: Wiley & Sons, 2001.