DNS欺骗攻击的检测与防御

李 建
(山西传媒学院, 山西 晋中 030619)

摘 要: DNS在为Internet的正常运行提供可靠保障的同时也遭受来自网络的欺骗攻击威胁, DNS攻击具有隐秘性强、打击面大、攻击效果明显的特点。文章分析了DNS系统解析流程、DNS欺骗攻击原理和分类, 并列出常见的欺骗攻击方式, 提出不同检测方法, 讨论了针对DNS欺骗攻击的防范策略, 对提高DNS抗欺骗攻击能力具有明显效果。

关键词: DNS欺骗攻击; 攻击模式; 检测方法; 防范策略

DNS(Domain Name System)为全球分布范围最广的分布式、多层次数据库系统, 提供从IP到域名间的映射服务, 是Internet正常运行的关键技术设施。DNS系统将便于识记的主机名映射为晦涩难记的IP, 并保障其他网络应用(Email投递、网站访问等)顺利进行。DNS系统一经提出即发展迅速, 全球注册主机数量从1987的2万余条发展到2005的3亿余条; 独立域数量也由1987年几个发展到05年8290万余个。截至2014年6月, 中国境内域名数达到1915万个。

DNS系统因其本身存在的脆弱性导致系统安全性、保密性均受到威胁, 随着网络快速发展, DNS面临越来越多的攻击威胁。2014年11月, ICANN(国际域名与IP地址分配管理组织)称其受到黑客攻击, 一批员工的账号、密码被盗, ICANN内部的“中央区域数据系统”中有关用户的姓名和地址信息以及与ICANN有业务往来的人士的个人信息也被盗。2014年1月21日, 全球顶级根域名服务器出现故障, 导致.com的网站无法访问。在Internet快速发展的今天, DNS重要性、安全性研究需求显得尤为突出。

1 域名系统解析原理

DNS系统分为根、顶级域名服务器、权威域名服务器、主机4个部分, 使用分布式数据库将IP地址和域名一一映射。

分析DNS欺骗攻击之前先界定其域名解析流程, DNS分为2个部分: Server(服务器端)和Client(客户端), 递归服务器内部已预先设置了根服务器的IP地址。DNS Server接受Client域名查询请求, 从DNS root逐层向下迭代查询。域名解析流程如图1所示(以访问www.phei.com.cn为例)。

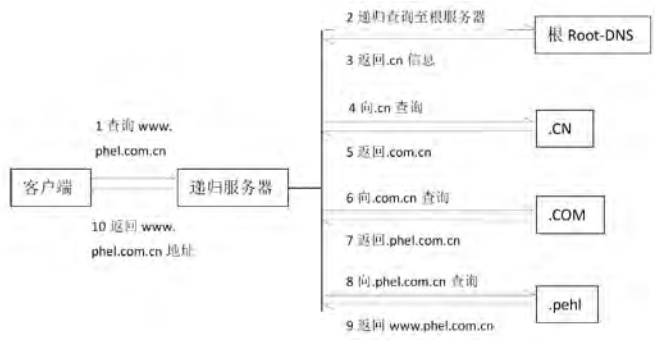

图1 域名解析流程

客户端首先向本地DNS服务器发出查询www.phel.com.cn的IP地址的请求, 如果本地DNS服务器在本机DNS缓存表中没有查到相关记录, 则立即向根服务器发起递归查询; 根服务器收到查询请求后, 将.cn域服务器地址反馈给本地DNS服务器; 本地DNS服务器继续向.cn域发出查询请求, 域服务器将.com.cn反馈给本地DNS服务器; 本地DNS服务器则继续向.com.cn域发出查询请求, 域服务器将phel.com.cn授权域名服务器的地址反馈给本地DNS服务器; 本地DNS服务器继续向phel.com.cn发起查询, 得到www.phel.com.cn的IP地址, 以DNS应答包的方式传递给用户, 并将查询所得内容复制在本地DNS缓存表中, 以备客户端查询。

2 DNS系统欺骗攻击原理

DNS域名系统安全性与Internet能否正常运行紧密相关, DNS系统遭受网络攻击时会造成重要信息被泄密、拒绝提供服务、网络服务瘫痪等事件发生, DNS安全性隐患包括以下几方面: (1)在设计协议时安全性考虑不足, 不能保证查询数据的真实性和完整性。(2)Internet在全球快速推广导致DNS系统信息管理难度增大, 系统冗余性降低。(3)针对DNS安全性问题提出的各种改进技术如DNSSEC、分布式哈希表等难以大范围使用。

DNS欺骗攻击是攻击者事先伪造为用户信赖的DNS Server, 将查询IP改为攻击者事先指定的IP, 进而将查询网站引向攻击者网站, 实施DNS Server域名欺骗攻击。此攻击方式主要包括2种: 缓存中毒、ID欺骗。

(1)缓存投毒。为尽最大可能地快速给用户提供服务, DNS Server将收到的Domain Name和IP地址映射数据保存至本地Cache, 保存期限TTL(TTL≥0), 在TTL不为0时, 如有访问该信息的请求信息, 无需重新查找可直接从本地答复, 此方式可高效利用缓存信息, 增强DNS设施服务效率。缓存机制的缺陷在于不检查附加数据, 缓存投毒攻击者利用此漏洞将TTL值设为较长时间即可实现长时间欺骗用户, 在TTL未失效内, 缓存内事先植入的虚假信息会快速扩散至其他DNS Server, 造成大面积缓存中毒事件发生。

(2)ID欺骗。当DNS缓存已记录的信息在缓存失效之前如有Client查询则直接返回缓存记录, 此过程使用Transaction ID与端口间的通信来标示一次通信过程。当进

作者简介: 李建(1979-), 女, 山西洪洞, 硕士, 讲师; 研究方向: 计算机网络, 大数据处理。

行域名解析时，Client用特定的ID标示向DNS Server发送解析数据包，DNS Server使用此ID向Client发送应答数据包，Client对比发送的请求数据包和应答数据包ID标示，如一致则说明该应答信息可靠，否则将该应答信息丢弃。

上述通信过程简洁明了，效率高，但易遭受攻击，如生日攻击。此攻击来自生日悖论，假设存在一个23人团队，则2人同一天生日的概率为50%。生日攻击利用此特点，向某一DNS Server请求同一域名查询时，也同时发送大量针对该域名不同ID的答复报文，增大了使该DNS Server的被骗几率。最常见的域名欺骗攻击是针对DNS数据报头部的事务ID进行欺骗。

3 常见DNS欺骗攻击方法

DNS常见欺骗攻击需要获取对方ID，主要有网络监听获取ID和序列号攻击（预测下一个ID）法。

（1）网络监听获取ID。为通过监听用户流量获得ID，攻击者可选择与DNS Server或众多客户端主机中某一主机位于同一局域网内。DNS系统允许在请求信息中添加额外信息，如IP地址、Domain Server等，Client接收到攻击的Domain Server查询请求时均被引向攻击者之前设定的Domain Server。因DNS系统仅用ID标示判定信息真实性，且ID从Client发出、由DNS Server返回，且客户端仅通过核实发出、返回端ID是否一致来确定信息的可靠性，使得通过网络监听的方式获取ID的攻击成为可能。

（2）序列号攻击原理。DNS查询报文格式中ID号所占位数为16位，即其取值范围为0~65535，其预测难度不大，该攻击过程中攻击者对正确报文DNS Server发起DDOS攻击，拖延DNS Server正确回复报文，保证攻击者的DNS Server抢在正确的DNS Server之前回复请求端报文，该报文内嵌ID与请求报文内嵌ID相同，Client接收先到的虚假报文，丢弃后到的真实报文。虚假报文中内嵌的IP将Client引向攻击者诱导的非法网站。

旧版BIND可通过较近几个DNS包ID来猜测虚假ID，新版BIND9利用上述猜测法成功概率有所下降，但其算法依然存在漏洞。据分析，通过新近收集到的5000个DNS包内的ID同样可成功测算出即将出现的下一个ID，成功率高达20%，因此，使用此方法伪造虚假ID并进行DNS欺骗攻击的成功率较高。

4 DNS欺骗攻击检测

有关学者提出多种检测DNS欺骗攻击方法，相关文献研究了Domain-Flux检测技术。恶意攻击软件使用的算法为DGA（域名生成算法），以time等参数为算子自动产生大量虚假域名并尝试连接与控制服务器。当发生DNS欺骗攻击时，Client将收到2个以上相同ID的应答报文，但只能有1个真实的应答报文，其余报文均为欺骗信息。但此类检测方法试用范围不同，鉴于此，本文提出检测方法。

4.1 被动监听检测法

被动监听检测法，检测接收的DNS应答报文，正常情况下应答报文只有1个，当域名与IP存在一对多的映射关系时，1个应答报文中将包含多个映射关系的回复，不会出现有多个应答报文情况。因此，如一个请求报文在额定时间内收到多个应答报文则有遭受DNS欺骗攻击的可能。

该检测法不会添加额外的网络流量负担，但因其检测方法的消极性无法检测出网络潜在攻击威胁。

4.2 主动试探检测法

主动试探检测法，由DNS系统主动发送检测数据包检测是否存在DNS欺骗攻击，通常主动发送的检测数据包不可能接收到回复，但攻击者为抢在合法数据包抵达之前能将欺骗包发给客户端，在不验证DNS Server的IP合法性情况下抢先发送应答报文，此情况发生说明系统受到DNS欺骗攻击。

主动试探检测法需要DNS系统主动发送大量探测包，容易增加网络流量负担、导致网络拥塞，且通常DNS欺骗攻击只针对特定域名，在选择探测包包含的待解析域名时存在定位性不强的问题，使得该方法的探测难度加大。

4.3 交叉检查查询法

交叉检查查询法，Client接收DNS应答包后反向对DNS Server查询应答包中返回的IP对应的DNS，如两者完全一致则说明DNS系统未受到欺骗攻击，反之亦然。

该查询方法介于前2种检测方法之间，即对收到的数据包在被动检测基础上再主动验证，依赖于DNS反向查询功能，但较多数量的DNS Server不支持此功能。

4.4 使用TTL（生存时间）DNS攻击检测

TTL（Time to live）位于IPV4包的第9字节占8bit，其作用是限制IP数据包在网络中的留存时间，在TTL不为0时，如有访问该信息的请求信息，无需重新查找可直接从本地答复。在进行DNS欺骗攻击时如需长时间欺骗则将TTL值设为较长时间即可。也是IP数据包在网络中可转发的最大跳数，即可避免IP数据包在网络中无限循环、收发，节约网络资源。通常同一Client发送的DNS查询请求会经过相对固定的路由、相对固定时间内到达DNS Server。即一定时间内，从同一Client发往固定DNS Server的请求数据分组TTL值大小是相对固定的。但网络攻击者发动的DNS反射式攻击需要不同地区的多台僵尸网络控制的受控计算机协同工作，同时发送虚假源地址的DNS请求信息，虽然攻击者可使用虚假的源IP地址、TTL等信息，但由于受僵尸网络控制的计算机分别位于不同地域，因此，真实IP地址对应的主机发送的数据分组抵达DNS Server的数量很难造假。

IP地址造假是成功实施DDOS攻击的必备条件，因此，使用TTL的DNS攻击检测方法可对来自相同源IP地址的DNS请求数据分组TTL值做实时对比，如相同源IP地址的TTL值变化频繁则可对DNS请求分组做无递归的本地解析或丢弃。使用此方法可发现假IP地址并有效遏制域名反射放大攻击。

5 防御技术

（1）遭受序列号攻击时可使用专业监听软件，正常情况下由DNS Server回复报文，如收到多个回复报文即怀疑有欺骗攻击；可从以下方面进行防御：仅仅授权自身管辖的域名解析提供递归查询，且只接受域外DNS Server的DNS查询请求，可减少遭到攻击的可能性；DNS重定向，所有到达DNS Server的查询均重定向至另DNS Server，对真实的用户提供正常域名查询功能，从而屏蔽、减少虚假IP造成的故障。

（2）缓存投毒特点是将TTL值变大，如发现TTL值过大需

重点关注。投毒攻击往往攻击银行、搜索网站、热门网站等，可将此类网站IP记录为相应表格，统计经常被请求解析的域名频率，记录域名查询失败次数，引入域名信誉机制，如请求IP与表中记录IP不一致则说明DNS回复信息可疑。

6 结语

网络攻击的检测和防范是推动网络进步的动力，本文分析了基于DNS构架的解析过程，阐述了DNS欺骗攻击原理，提出针对DNS欺骗攻击的检测方法和防范方案，对提高DNS系统抗欺骗攻击能力和安全性有积极作用。随着网络的快速发展后续还需进一步探索更有效的检测方法，以提高DNS系统抵御各种新型欺骗攻击的能力，保证系统安全、稳定地运行。

[参考文献]

[1]天极软件频道.互联网管理机构ICANN遭攻击部分资料被泄露[EB/OL].[2014-12-22]. http://soft.yesky.com/security/348/42849348.shtml.
[2]前瞻网.1月21日网络故障:根域名服务器dns遭黑客攻击致网络瘫痪[EB/OL].[2014-01-22].http://www.henan100.com/news/2014/328895.shtml.
[3]YADAV S, REDDY A K K, REDDY A L N, et al.Detecting Algorithmically Generated Malicious Domain Names[C]//In 10th ACM SIGCOMM Conference on Internet Measurement, Melbourne, Australia, November1-3, 2010.
[4]ANTONAKAKIS M, PERDISCI R, NADJI Y, et al.From Throw-Away Traffic to Bots Detecting the Rise of DGA-Based Malware[C]//In 21st USENIX Security Symposium, Bellevue, WA, USA, August 8-10, 2012.
[5]YADAV S, REDDY A L N.Winning with DNS Failures: Strategies for Faster Botnet Detection[C]//In 7th International ICST Conference on Security and Privacy in Communication Networks, London, UK, September 7-9, 2011.
[6]YADAV S, REDDY A K K, REDDY A L N, et al.Detecting AlgorithmicallyGenerated Domain-Flux Attacks with DNS Traffic Analysis[J].IEEE/ACMTransactions on Networking, 2012(5):1663-1677.

Detection and Prevention of DNS Spoofing Attacks

Li Jian
(Communication University of Shanxi, Jinzhong 030619, China)

Abstract: When providing reliable guarantee for the normal operation of the Internet, the DNS is also spoofing attacks from the network. The DNS spoofing attacks are obvious characteristics with the strong privacy, larger surface combats and good attack effects. The paper analyzes the workflow of the DNS system, the principle and classification of the DNS spoofing attacks, and lists the common spoofing attacks, proposed different methods. And discussed the prevention strategies for the DNS spoofing attacks. These methods have obvious effects to improve the anti-spoofing capabilities of DNS.

Key words: DNS spoofing attacks; attack mode; detection method; prevention strategies