DNS 欺骗攻击的检测和防御措施探究

李祉岐 宋 洁 曹明明 王 杨
(国网思极网安科技(北京)有限公司,北京 100000)

摘 要:DNS 是当前网络应用基础,对 DNS 所进行的攻击会对 Internet 运转产生影响。DNS 欺骗攻击作为攻击者最为常用的一种手段,其具备了打击面广、隐蔽性强和攻击效果显著的特征,可是现在对于这种攻击手段缺少防御措施。本文系统阐述了 DNS 欺骗攻击的原理,并以此为基础探究了 DNS 欺骗攻击所采用的方式与手段,最后提出了 DNS 欺骗攻击的检测以及防御措施。

关键词:DNS 欺骗;检测;防御
中图分类号:TP393.08 **文献标识码**:A **文章编号**:2096-4390(2019)04-0069-02

DNS 是一种域名命名系统,人们可以借助 DNS 将机器名称转变为 IP 地址,从而确保所有的用户都能够使用网络。在网络应用中输入 DNS 名,DNS 服务器当中的数据库就能够提供包含 IP 地址在内的所有和名称相关的内容。比如,在浏览 WEB 的时候, 人们经常采用 microsoft.com 这类的名称实现对计算机的定位,可是计算机直接通讯的时候采用的通常是数字地址。为了妥善的解决该问题,能够采用 DNS 将字符名称映射到计算机实际数据地址。

长久以来,很多学者都在研究 DNS 的安全性,并针对 DNS 本身所存在的缺陷而言提出了多种多样的解决方法。比如 IETF 安全工作组针对 DNS 所存在的弊端, 提出了 DNSSEC 协议,其增设了认证机制,加强了协议安全性。可是,目前该协议在密钥管理以及系统效率等方面依然存在诸多问题,距离大规模的应用和普及尚存一定距离。所以,除了研究 DNS 协议安全以外,很多文章以当前 DNS 协议为此基础,提出了安全防范方案,升级了服务器软件,对 DNS 系统配置进行了优化,有效解决了 DNS 协议本身所存在的问题。但是依然有一些无法避免的攻击存在,比如 DNS 欺骗攻击,对于这类攻击还没有很好的解决方法。

1 DNS 欺骗攻击原理

比如,当客户想要访问 www.dhs.com 网站的时候,需要先获得该网站的 IP 地址。客户主机得到该 IP 地址的唯一手段是查询其当前所处的 DNS 服务器,查询的过程可以分成四个步骤:

第一,客户主机向 nipc.com 域 DNS 服务器发送请求,要求其对 www.dhs.com 进行解析,nipc.com 接到请求以后, 对 dhs.com 域 DNS 提出解析请求,dbs.com 接收到请求以后给予解析应答,nipc.com 将解析应答转存在本地缓存中。

DNS 欺骗攻击主要发生在客户主机箱本地 DNS 服务器进行域名查询的过程中, 假如服务器缓存当中已经存 (转下页)

练者或教练员发出的特定的语言指令, 进行后台分析处理,进行随机发球,训练者则做出相应的接球和投球等动作,以起到训练球员的目的。

3.3 大数据技术:机器人可通过安装的视觉识别系统以及专业评估系统,对运动员的接球、投球或者踢球动作进行数据采集、分析和处理,总结分析形成报告单,为运动员的练习提供更为科学有效的改良建议。

3.4 机械自动化技术:这是一门综合性技术,其中又以控制理论和计算机技术对自动化技术的影响最大。考虑到实现机器人运动状态、图形图像实时传输、夹持状态等各状态下的自动化,此技术是制造过程当中最关键的一环。

4 大球类球场机器人的社会意义与发展前景

大球类球场机器人是社会进步和科学技术进步的产物, 也是市场竞争、产业升级的必然结果。 不管是对于用户、企业、还是社会都具有重要的意义。首先, 对用户来说, 球场机器人在满足其基本使用需求的同时, 更加注重在使用的过程中所带来的智能化、专业化、个性化服务;其次, 对于企业来说, 大球球场机器人是一个很好的创新突破点, 它可以极大的提高企业在激烈的市场竞争中的地位, 使企业处于行业的领先位置。

5 结论

随着人们生活水平的日益提高, 人们对自身的健康以及休闲时间的娱乐质量有了越来越高的要求。如何将高效的机器人应用于训练者的日常陪练和服务,以减轻当前陪练人员劳动强度大、解决效率低下,以及降低训练者的训练成本和开发更多娱乐潜能等,成为当前球场机器人的热点问题。大球球场机器人是科学技术的进步和人类发展的必然结果, 它的发展必将极大的丰富人们的生活,为社会创造了大量的价值。同时也开阔了我们的视野,让我们对自身、对生活方式有了新的思考与认识,未来可期。

参考文献

[1]赵京,张自强,郑强,等.机器人安全性研究现状及发展趋势[J].北京航空航天大学学报,2018,(7):1347-1358.
[2]关慧贞,高英明.一种手控拾发球机器人的设计[J].机床与液压,2004,(12):141-143.
[3]张欣.智能乒乓球发球机器人[D].厦门:厦门大学,2014.
[4]张昊龙.移动机器人图像处理关键技术研究与实现[D].电子科技大学,2017.
[5]许玉虎.基于虚拟样机技术的协作机器人运动学与动力学研究[D].泰安:山东农业大学,2017.
[6] 篮球百度百科.https://baike.baidu.com/item/%E7%AF%AE%E7%90%83/123564?fr=aladdin.
[7]足球百度文库.https://wenku.baidu.com/view/dca60de085868762caaedd3383c4bb4cf6ecb719.html.
[8]排球百度经验.https://jingyan.baidu.com/article/11c17a2c4ed75bf447e39d41.html.
[9]机器人发展简史:看看机器人的前世今生.http://robot.ofweek.com/2017-01/ART-8321203-8420-30097781.html.2017.

作者简介:刘兰馨(1997,2,26-),女,安徽阜阳人,昆明理工大学艺术与传媒学院工业设计专业学生。

在相对应的记录,DNS 服务器就不会再向其他的服务器提出查询请求,而是会将该条信息直接反馈给用户主机。但是入侵者想要完成 DNS 欺骗,就需要在本地 DNS 服务器 cache 当中预设一条伪造解析记录。此时当 dhs.com 域 DNS 将这条预设的虚假信息返回给 nipc.com 的时候,nipc.com 域 DNS 服务器就会接受该结果,并且会把这个错误的信息存储在本地的 cache 当中。以后这条缓存记录存在期间内,向 nipc.com 域的 DNS 服务器所发送的 www.dhs.com 域名解析请求,获得的 IP 地址都被修改过。

总而言之,不论使用何种方法进行 DNS 欺骗攻击,最终的结果都是将用户引入攻击者所期望的网站当中。

2 DNS 欺骗攻击的方式

当前,DNS 欺骗攻击的形式包含了两种,分别是内应攻击、序列号攻击。其中内应攻击指的是攻击者侵入并且控制 DNS 服务器,修改数据库当中的域名,把域名对应的 IP 地址转变为攻击者预设的 IP 地址,在主机用户想要查询该域名的时候,所得到的就是攻击者所预设的虚假域名。这种攻击方式在实施的过程中通常需要攻击者具备相对较高的技术,同时也可以经常接触 DNS 服务器。而序列号攻击则是采用 DNS 服务器当中的漏洞进行攻击。在 DNS 协议当中,域名请求与应答数据包都是通过序列号进行匹配的。攻击者能够假扮成 DNS 服务器,将带有请求包序列号的应答数据包传送到主机用户手中,并且在真实应答数据包到达之前转送到主机客户端。此时,主机用户查询的相关域名对应 IP 地址便是攻击者所指定的假地址,用户也就自然而然的被带到了攻击者所预设的网站当中。

3 DNS 欺骗攻击检测手段

相关学者提出了很多种 DNS 欺骗攻击的检测方法,比如被动监听检测法、主动试探检测法、交叉检测查询法等方面,本文将做一一说明。

3.1 被动监听检测法

该方法对 DNS 应答报文进行检测接收,普通情况下,通常只有 1 个应答报文,在域名以及 IP 存在一对多映射的情况下,1 个应答报文会包含多个映射关系,此时不会出现多个应答报文的情况。所以,如果一个请求报文在特定时间里获得了多个应答报文,那么就可能遭到了 DNS 欺骗攻击。这种检测手段不会增添额外网络流量负担,可是因为检测手段消极性,难以检测出网络当中暗藏的攻击威胁。

3.2 主动试探检测法

该方法主要是 DNS 系统发送检测数据包,最终实现对 DNS 欺骗攻击的检测。一般检测数据包并不能接收恢复,可是攻击者为了能够在合法数据包到达之前将欺骗数据包发到指定的位置,在没有验证 DNS Server 的 IP 合法性的时候抢先发送了应答报文,此时就表明系统遭受到了 DNS 的欺骗攻击。该方法要求 DNS 主动发送探测包,会提升网络流量负担,造成网络拥堵,并且一般 DNS 欺骗攻击针对的是特定的域名,在选择探测包所包含的各种待解析域名的时候存在定位性较低的问题,提升了检测的难度。

3.3 交叉检查查询法

交叉检查查询法指的是客户在获得 DNS 应答包以后,反向查询 DNS 服务器应答包当中返回 IP 地址所对应的 DNS 名称,假如二者保持一致,那么就表明其没有受到攻击,否则的话就代表受到了攻击。

上述三种方法中,被动监听检测是一种被动的方法,主动试探检测以及较差检查查询两种方法是主动检测的方法。被动监听检测不会产生额外的网络流量,但是其本身是一种消极应对的方法,很难检测出潜在攻击。而主动试探检测的方法则会向发送额外的探测包,从而增加了网络负担。除此之外,DNS 欺骗攻击一般只能够欺骗特定的域名,这种探测包中对于待解析域名所进行的选择本身就存在不确定性,增加了探测难度。交叉检查查询法介于两种方法之间,采用的是反向查询的方法,实现对 DNS 欺骗攻击的检测,但是很多 DNS 服务器并不具备发现查询的功能,因此该方法实施起来存在一定的难度。

4 DNS 欺骗攻击防御措施

当发现 DNS 欺骗攻击后,要使用相对应的防御措施。由于 DNS 序列号攻击是依托 ARP 欺骗攻击实施的,因此,假如可以对 ARP 欺骗攻击行为进行防御,那么也就能够组织 DNS 序列号欺骗攻击。具体的防御措施包括以下几种。

第一,主机用户绑定 IP 地址以及 MAC 地址,这种做法可以避免 ARP 欺骗行为的发生,进而对 DNS 欺骗攻击具备一定的抵御效果。

第二,DNS 欺骗攻击通常会对 DNS 服务器当中的 IP 地址进行更改,最终实现其欺骗攻击的目的。但是,每个网卡都会对应位移的 MAC 地址,为此,我们可以绑定 DNS 服务器中的 IP 地址以及 MAC 地址,将其存储于主机客户端的网卡 Eprom 中。当客户得到 DNS 服务器应答数据之后,检测其中所包含的 MAC 地址和我们在 Eprom 存储器当中的数据是否吻合,如果二者之间存在差异性,那么就可以将应答数据包丢弃。

第三,为了避免 DNS 欺骗攻击的行为发生,对于一些信息安全性相对较高的网站能够直接采用 IP 地址对其访问,由于有些 DNS 欺骗攻击的最终目标是针对用户隐私数据,这样做能够降低因为 DNS 欺骗所产生的损失。

结束语

总而言之,从某种意义上看,网络安全的发展是以网络攻击为推动力的。对于 DNS 攻击,要注重对新的检测与防御技术的研发,有效提升 DNS 安全性,使得网络环境更加的有序、健康。所以,本文对于 DNA 欺骗攻击行为的研究,有助于净化网络环境,推动网络进一步发展。

参考文献

[1]肖瑶瑶,肖庚生,刘朝晖.抵抗基于 DNS 欺骗网页克隆攻击方案的研究[J].湖南理工学院学报(自然科学版),2018,31(3):36-40.

[2]罗玉梅.典型网络欺骗攻击原理及防范的研究[J].电脑知识与技术,2016,12(11):36-37.

[3]宋庆福.TCP/IP 协议下常见网络攻击技术及其防范[J].科技信息(科学教研),2008(5):79,72.

[4]刘扬,刘杨,胡仕成,朱东杰.基于 ARP 与 DNS 欺骗的重定向技术的研究[J].计算机工程与设计,2007(23):5604-5606,5609.

[5]闫伯儒,方滨兴,李斌,王垚.DNS 欺骗攻击的检测和防范[J].计算机工程,2006(21):130-132,135.

[6]龚坚,李坚石.RSA 加密在 DNS 安全中的应用[J].贵州大学学报(自然科学版),2005(1):51-54.