

基于免疫网络的 ARP 攻击防御方案研究与实施

王晓妮¹, 韩建刚²

(1. 咸阳师范学院 信息中心, 陕西 咸阳 712000;
2. 西北机电工程研究所电调室, 陕西 咸阳 712000)

摘要: ARP 攻击是利用 ARP 协议设计时缺乏安全验证漏洞来实现的, 通过伪造 ARP 数据包来窃取合法用户的通信数据, 造成影响网络传输速率和盗取用户隐私信息等严重危害。为了解决校园网中难以彻底清除的 ARP 攻击现象, 提出了一种基于免疫网络的 ARP 防御方案。通过研究 ARP 协议及其工作原理和 ARP 攻击引起的危害及其攻击原理, 采取免疫网络技术来防御校园中的 ARP 攻击欺骗。经过分析用户需求和方案设计思想, 设计了方案的技术架构和体系架构, 部署并实现了免疫网络防御方案。对该方案在校园网中进行了应用测试, 经过实验比较分析, 结果表明免疫网络方案比目前常见的 ARP 防御措施的防御效果更好, 能够很好地监控和防御校园的 ARP 病毒, 解决了目前存在的无法彻底根除 ARP 攻击欺骗防御技术的瓶颈。

关键词: 校园网; ARP 协议; ARP 攻击; 免疫网络

中图分类号: TP393.18

文献标识码: A

文章编号: 1673-629X(2019)04-0095-05

doi: 10.3969/j.issn.1673-629X.2019.04.020

Research and Implementation of ARP Attack and Defense Scheme Based on Immune Network

WANG Xiao-ni¹, HAN Jian-gang²

(1. Information Center, Xianyang Normal University, Xianyang 712000, China;

2. Electrical Debugging of Northwest Institute of Mechanical and Electrical Engineering, Xianyang 712000, China)

Abstract: ARP attack is realized by the lack of security verification loopholes in the design of ARP protocol. It steals the communication data of legitimate users by forging ARP data packets, causing serious harm such as affecting the network transmission rate and stealing user privacy information. In order to solve the problem of ARP attack in campus network, we propose an ARP defense scheme based on immune network. By studying the ARP protocol and its working principles, and the harm caused by the ARP attack and its attack principle, the immune network technology is adopted to prevent the ARP attack fraud in the campus. After analyzing the user requirements and the design idea of the scheme, the technical framework and architecture of the scheme are designed, and the immune network defense scheme is deployed and implemented. This scheme has been tested in the campus network. The experimental comparison and analysis shows that the proposed scheme has better defense effect than the common ARP defense measures. It can monitor and defend the ARP virus of campus well, and solve the bottleneck of the existing technology that can not completely root apart the ARP attack deception defense technology.

Key words: campus network; ARP; ARP attack; immune network

0 引言

随着网络通信和计算机技术的飞速发展, 人们的工作和生活离不开网络, 整个社会已进入信息时代, 担任国家信息化建设重要任务的高校责无旁贷, 智慧校园应运而生^[1]。校园网对高校的科学研究、行政管理、人才培养、学科建设和师生工作学习及日常生活等方

面产生了深远的影响, 已成为学校的重要基础设施。然而高校信息化建设的快速发展和校园网用户的急剧增加, 使网络安全问题变得尤为突出, 最为常见的欺骗攻击便来自于 ARP 病毒。其破坏力非常大, 它的危害程度在所有电脑病毒中位居第五, ARP 欺骗攻击已严重威胁校园网的安全, ARP 病毒的防御问题已引起广

收稿日期: 2018-05-08

修回日期: 2018-09-12

网络出版时间: 2018-12-19

基金项目: 陕西省教育科学“十三五”规划 2017 年课题 (SGH17H196); 咸阳师范学院专项科研基金资助项目 (13XSYK087)

作者简介: 王晓妮 (1977-), 女, 硕士, 工程师, 研究方向为计算机应用和网络安全。

网络出版地址: <http://www.cnki.net/kcms/detail/61.1450.TP.20181219.1553.086.html>

大高校网络管理人员的高度重视^[2]。文中分析了常见的 ARP 欺骗防御措施存在的不足,并提出免疫网络以解决高校局域网中的 ARP 欺骗攻击。

1 ARP 攻击原理和危害

ARP(address resolution protocol, 地址解析协议)是一个根据主机 IP 地址获取其 MAC 地址的 TCP/IP 协议^[3]。在 IPV4 网络环境中会为每台设备分配一个固定的 IP 地址,可是如果两台主机想在以太网中直接通信,源主机仅知道目标主机的 IP 地址是无法实现的,必须知道其 IP 地址对应的 MAC 地址(唯一标识),而这个 MAC 地址只能通过 ARP 协议获取^[4]。ARP 协议的工作原理^[5]见图 1。因为 ARP 协议在起初设计时没有考虑到其安全性,它是以 LAN 中所有设备都相互信任和安全为基础来实现的。虽然 ARP 协议保证了数据传输的便捷高效,但是其自身却存在广播性、无认证、动态性和无状态这些安全漏洞^[6]。

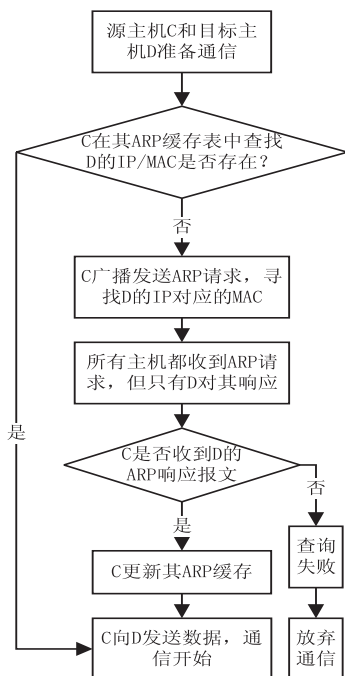


图 1 ARP 协议工作原理

ARP 欺骗攻击就是黑客利用 ARP 协议的这些漏洞,把自己的 MAC 和想要截获数据的目标设备的 IP 构成 IP/MAC 发送给源主机,冒充目标主机去响应 ARP 请求,让收到响应的源主机更新其 ARP cache,这样就让本该发送给目标主机的数据发给了黑客。ARP 病毒欺骗原理如图 2 所示。校园网中出现了 ARP 攻击欺骗现象,病毒主机就会向网络中发送大量的数据包,造成网络拥塞,出现用户打开网页很慢甚至根本无法打开的现象^[7],接着发现整个校园网中病毒的网段内的主机不停提示 IP 地址冲突、网速奇慢无比、频繁断网、不停有恶意广告弹出、重启设备、网卡禁用或更

换新的 IP 后网络就会恢复短暂的正常^[8]。

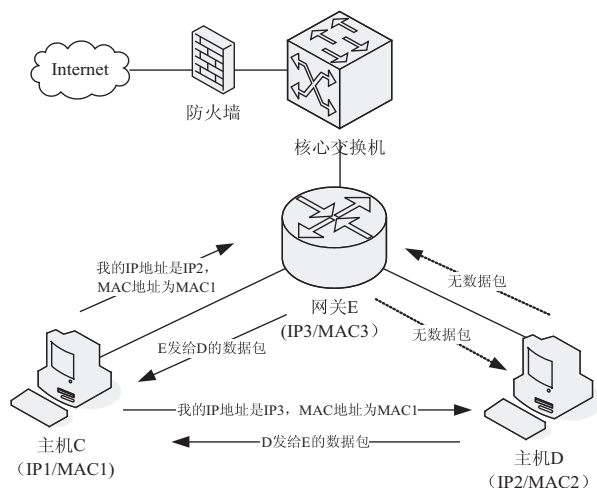


图 2 ARP 欺骗网关攻击原理

2 基于免疫网络的 ARP 欺骗攻击防御方案设计

2.1 需求分析

目前 ARP 欺骗防御措施虽然很多,但用户仍旧无法彻底摆脱 ARP 欺骗攻击的困扰,主要是因为常见的防御措施存在诸多不足^[9]。双向静态绑定虽能有效防止普通的 ARP 欺骗攻击,但仅适用于较小规模的局域网,一旦更换上网地点绑定就会失效^[10]。VLAN 划分由于缺乏保护网关的措施,即使 VLAN 划分的再细,一旦网关遭受了 ARP 攻击就会前功尽弃。ARP 防火墙无法识别所绑网关的正确性,无法解决 ARP 攻击造成的危害,故存在一定的风险^[11]。交换机端口绑定必须利用那些带有 MAC 学习功能的交换机,其价格很高,这就加大了网络投资成本^[12]。ARP 服务器法必须保证 ARP 服务器的安全性,这就成了整个校园网的瓶颈,稍有不慎就会全网瘫痪。采用 PPPOE 计费方式虽能避免其遭受 ARP 欺骗,但由于封装和解封装操作降低了网络传输率,该技术使局域网间无法访问和共享网络资源^[13]。故现有 ARP 防范措施都存在一定的问題,虽然对 ARP 进行了非常深入的研究,但依然在实践中无法彻底解决。因此,免疫网络防御方案应运而生。在校园网中组建免疫网络系统成本不是很高,因为所使用的网络设备和以往传统设备价位差不多,但在性能上却有很大的优越性^[14]。可见采用免疫网络来防御 ARP 欺骗的方案在技术上是可行的。

2.2 设计思想及目标

该方案的设计思路是网络问题靠网络手段去解决,其核心是免疫墙,利用其免疫机制来控制管理内网的传输层和链路层操作,实现内网安全管理防御 ARP 攻击。此方案通过控制中心、驱动程序、免疫路由器和

服务器等软硬件相结合的独特技术架构,利用先天免疫技术来实现网关的主动防御机制和独特的 NAT 处理机制这两种有效技术措施,提前制定好相关的免疫策略来控制校园网,从多角度立体化防御 ARP 攻击。

该方案的设计目标是通过免疫网络技术来对校园网进行内外兼顾和软硬兼施综合管理,采用免疫路由器、用户终端上网驱动程序和监控中心三者结合,对校园网运行状况全面掌控。它打破了原来网络被动防御的局限,立足局域网内部,联动所有网络设备、提高接入设备的可信度、增强了防御和控制措施、细化带宽和业务管理和提高整个网络的监测评估,更好地解决目前多样复杂的网络攻击和威胁。

2.3 技术架构设计

免疫网络原指自然界的生物体内连锁发生的那些自我识别过程,现指让互联网具备了类似人体的监视、防御和稳定的功能^[15]。它运用了自我管理和防御的理念,将全网联动、群控群防和源头抑制这些措施充分利用在网络中的所有节点,增强了其安全性,使其面对各种攻击应对自如。免疫网络防御体系是一套针对局域网底层防火墙,其核心是构造出类似于人体神经控制网络技术的架构,把它的神经末梢渗透到网络的各部分。免疫网络通过免疫路由器管控局域网中的所有用户主机,每个用户主机的网卡驱动层都安装了上网驱动程序,防止非法用户的不安全接入。网络中的所有设备和主机的驱动程序使其具有探测功能,通过探测流经本机上的网络信息并将它发送到免疫监控中心,该探测信息包含设备信息、异常流量和事件等。免疫监控中心收到探测信息后根据规约库中的控制策略对此做出响应并返回相应的指令,并给出相应的防御措施和警告信息。网络设备和主机根据监控中心的响应指令,通过免疫驱动程序采取措施拦截或清除非法传播的错误网关信息,阻止其进入用户主机,避免终端用户主机发起 ARP 攻击。

人体免疫系统需要分辨“敌我”,同样免疫网络防御体系也需要。在免疫网络防御体系中,只允许符合条件的客户端设备接入网络,直接拦截和隔离来自非法用户的数据包,对所有的网络设备和数据报文通过免疫监控中心来控制。此方案采用的核心设备是欣向 NuR8528G+免疫路由器,IBM 服务器,其操作系统是 Server 2008,数据库采用 SQL Server 2005。首先要建立认证接入的基础架构,保证各种应用的安全传输;其次检测出异常信息后应及时拦截和清除,尽可能减少 ARP 攻击;最后要建立信任的身份认证和管理体系,利用免疫驱动程序来实现合法用户的身份认证,确保上网用户的 IP/MAC 真实有效,用户的所有上网数据都必须经过驱动程序,这样便能有效防范 ARP 攻击。

2.4 体系架构设计

利用免疫网络与人体结构防御体系相对应的特点来设计方案的体系架构。该方案采用 C/S 体系架构,主要由服务器端、免疫路由器、内网安全协议和客户端这几部分组成。防火墙、物理网闸等网络的隔离设备对应于人体的表皮层,交换机、路由器等网络设备对应于人的神经层,服务器和用户计算机等主机设备对应于人的体内组织。利用控制中心和通信协议将各组成部分联动起来,全方位地遏制网络安全威胁。服务器端包括免疫服务器、免疫监控中心,策略库和 Webserv-er 等免疫服务组件,主要负责资源存储、审计监控、发布控制策略、安全管理控制和应用服务等操作,实现统一管理网络终端和网关,确保校园网内部协议稳定安全。客户端包括用户上网驱动程序,主要向服务器发送请求和执行来自服务器端的安全管理控制策略,避免用户主机遭受其他网络设备的攻击及自身攻击其他主机。内网安全协议负责服务器端和客户端间的通信,将服务器、客户端上网驱动程序、免疫墙路由器、免疫监控中心等这软硬件资源有机结合在一起,实现各部分的联动控制和信息共享。免疫网络防御体系具体的体系架构如图 3 所示。

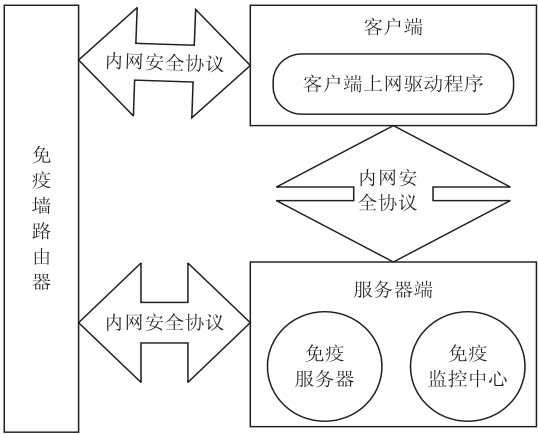


图 3 免疫网络体系架构

3 方案部署及实现

该方案采用软硬件相结合的方式在校园网中搭建了一个可靠稳定的基础网络平台,提供整体内网基础架构免疫服务来实现统一策略和安全管理,能够有效防御 ARP 攻击欺骗的发生。组建方式类似于传统的校园网,在校园网中具体部署该方案的免疫网络拓扑结构如图 4 所示。部署过程如下:首先将普通网络结构中的宽带接入设备用免疫网关或免疫墙路由器代替,根据校园网管理的实际需求,把相应的免疫策略和 IP 管理措施在免疫网络设备上规划好;其次加入一台始终运行免疫中心软件和自带网关的免疫服务器;要求所有用户安装客户端的上网驱动程序,否则就无法

上网。

具体实现过程如下：

(1)客户端。在免疫模式下,校园网用户必须通过免疫网关上网。所有用户必须安装记录了网关 MAC 地址的上网驱动程序,实现对 IP/MAC 的看守式绑定,把正确的网关 IP/MAC 地址合理存储和保护,杜绝网关的非法更改,就能够避免 ARP 欺骗的发生。

(2)服务器端。网管人员首先确定校园网用户的真实身份,利用驱动程序将其真正的 IP/MAC 和免疫标识整合在一起形成数据包,防止篡改和假冒。网管员信息中心的运行室能够通过免疫监控中心对所有用户上网行为随时监控和管理,变被动防御为主动出击,及时发现 ARP 病毒引起的异常设备并把攻击消灭在萌芽状态。

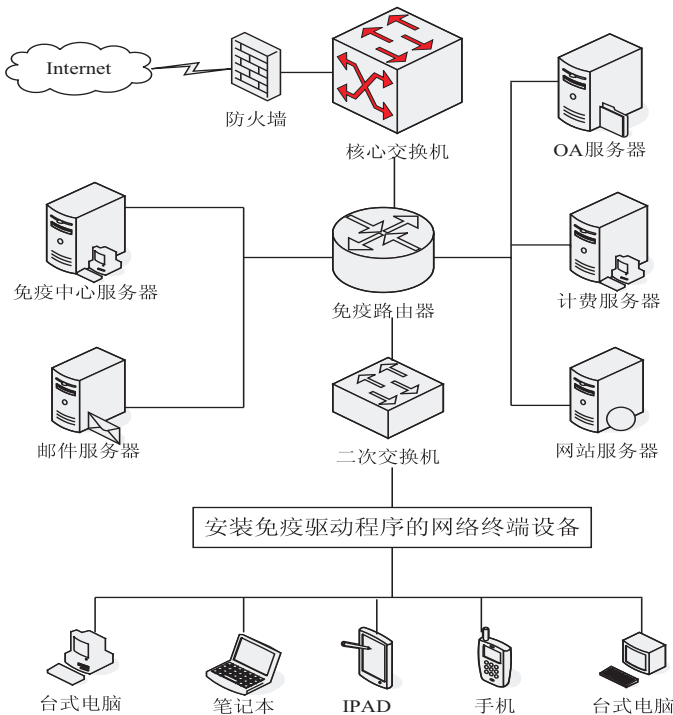


图 4 免疫网络拓扑结构

(3)免疫墙路由器。首先要对局域网用户的 IP 地址进行 NAT 转换,在进行 NAT 时改变了算法,加入了特殊的机制和安全措施,在 IP 转换过程中网关自动将用户主机的 MAC 地址记录在它的 NAT 表中,丢弃了往常的 NAT 映射 IP/MAC 算法,拒绝处理所有对终端 IP/MAC 列表的 ARP 请求,避免了处理 ARP 请求,使 ARP 病毒对免疫网络失效。这既从根本上杜绝了内网中出现 ARP 攻击欺骗网关现象的发生,又能节省 IP 地址。针对该校的具体情况,对不同的区域采用的不同的 NAT 路由配置方法。例如校内专用服务器 (Web、邮件、FTP、DSN 等) 和防火墙 DMZ 接口均采用静态 NAT,将其私有 IP 地址转化为固定的公有 IP,便于校外用户对这些特定设备的访问。而在用户数相对松散的行政办公区、综合教学楼、后勤集团、校医院、附中和幼儿园等采用动态 NAT,将这些用户的私有 IP 地址转化为不确定的公有 IP,可缓解 IP 地址紧缺的压力。而在用户密集和 ARP 攻击泛滥区如学生公寓楼、家属楼、各系部实验室、多媒体教室和阅览室采用端口复用动态 NAT,改变外出数据的源端口并加以转换,既能节省 IP 地址,又能防御外网攻击。

现以办公楼为例来进行端口复用动态 NAT 路由配置,共分四步:首先设置外部和内部端口;然后定义合法 IP 地址池和内部访问列;接着改变算法和机制,并加入安全措施;最后设置复用动态地址转换。对应的部分命令语法如下:interface serial/ethernet 0;ip address ip 地址值 + 网关;ip nat outside/inside;interface ethernet 0;ip nat pool 地址缓冲池的名称 ip 地址范围 netmask 子网掩码;access-list 1 允许访问的互联网的网段范围;ip nat inside source list 访问列表号 pool 内部合法地址池名称 overload。

4 方案测试及应用效果

4.1 方案测试

由于校园网结构复杂,用户数量大,故选择图书楼来进行方案测试,具体的测试环境如下:信息中心运行室北电核心交换机一台,免疫路由器一台,各楼宇间的锐捷汇聚交换机和接入交换机数台,免疫中心服务器使用 IBM 服务器一台,图书楼中的用户主机数台。该系统 C/S 结构的客户端驱动程序安装在用户主机上,免疫中心服务器端部署在 IBM 服务器上。

4.2 应用效果

在校园网中部署了免疫网络技术方案后,能够盘查到互联网的出入口、总揽到校园网的全貌、拓展到校园网的最末端和入到网络协议的最底层,很好地监控

和防御了该校的 ARP 病毒。通过测试可知,对免疫网络防御 ARP 攻击欺骗方案与目前 ARP 病毒常见的防御策略在具体应用中对技术指标进行了详细对比,其结果见表 1。

表 1 ARP 欺骗攻击防御措施技术指标对比

技术指标	双向绑定	交换机端口绑定	划分 VLAN	ARP 服务器	PPPOE 技术	ARP 协议改造	ARP 防火墙	免疫网络
维护方便	×	×	√	√	√	√	×	√
安全可靠	√	√	×	×	√	×	√	√
操作简单	×	×	√	√	×	×	×	×
部署成本低	√	×	×	√	√	×	√	√
适用范围广	×	×	×	√	×	√	√	√
工作效率高	×	×	×	√	√	×	×	√
防御效果好	√	√	×	×	√	√	√	√
统计结果	×	4	5	5	2	2	4	3
	√	3	2	2	5	5	3	4
技术指标达标率/%	42.9	28.6	28.6	71.4	71.4	42.9	57.1	85.7

从表 1 对比结果中可知,其他防御措施的技术指标达标率大部分在 28.6 % ~ 71.4 % 之间,只有免疫网络高达 85.7 %,由此说明该方案的技术指标已达标。由于客户端要安装免疫驱动程序,因此不可避免地影响用户上网操作,但其安装过程简便,速度很快几乎可以忽略不计,对该方案的整体性价比和实用性影响不大。

5 结束语

在高校局域网中组建免疫网络系统后,能够将外网的出入口检测到、对内网的各个角落一览无余、对协议的最底层和网络的最末端触手可及,使整个校园网的免疫力得到提高,全面抵御校园网中的 ARP 病毒攻击。使网络管理员能够随时监控校园网内所有设备的运行细节,特别是对终端用户设备的管理做到方便可控,能够全面抵御网络病毒,对 ARP 病毒防患于未然。较之六种常见的 ARP 病毒防御措施,免疫网络具有严谨的技术、可行的应用、低廉的成本等优点,使它能够很好地解决 ARP 欺骗攻击。作为网络技术前沿发展阵地的高校,拥有丰富的人力资源和国家大力支持的科研经费,这就为免疫网络在高校中的推广和深化提供了有力的保障。故在高校中搭建免疫网络系统,为校园网的安全运行提供有力保障。

参考文献:

[1] 任 皓. 基于 Wireshark 的 ARP 欺骗分析及发现技术[J]. 电子设计工程, 2018, 26(2): 18-21.

[2] 王晓妮. 高校局域网中 ARP 攻击防御策略的分析与实施

[J]. 航空计算技术, 2017, 47(3): 125-129.

[3] 李延香, 袁 辉, 刘淑英. 校园局域网 ARP 欺骗攻击的防御方法和实施[J]. 自动化与仪器仪表, 2015(9): 215-217.

[4] 任 侠, 吕述望. ARP 协议欺骗原理分析与抵御方法[J]. 计算机工程, 2003, 29(9): 127-128.

[5] 许力文, 乔丽娟. 基于大型校园网的 ARP 病毒防范[J]. 计算机光盘软件与应用, 2010, 11(3): 23-24.

[6] 黄天福, 白光伟. 基于改进协议机制的防 ARP 欺骗方法[J]. 计算机工程, 2008, 34(14): 168-170.

[7] 徐智勇, 吴自友, 蔡 聪, 等. 基于 Dynamic ARP Inspection 的静态 MAC-IP 绑定——一种 ARP 欺骗避免的解决方案[J]. 测控技术, 2013, 32(10): 93-97.

[8] 唐秀存, 王国欣. 基于 ARP 欺骗内网渗透和防范[J]. 计算机与信息技术, 2007(4): 40-42.

[9] 秦丰林, 段海新, 郭汝廷. ARP 欺骗的监测与防范技术综述[J]. 计算机应用研究, 2009, 26(1): 30-33.

[10] 刘 坤. 基于 Snort 的校园网 ARP 欺骗检测应用研究[J]. 计算机安全, 2011(7): 61-63.

[11] 郑森森. 基于 ARP 欺骗的数据截获与高速转发技术研究[D]. 成都: 四川师范大学, 2015.

[12] 李海鹰, 程 灏, 吕志强, 等. 针对 ARP 攻击的网络防御模式设计与实现[J]. 计算机工程, 2005, 31(5): 170-171.

[13] WU Lei, GU Qiwei. Windows network packet capture technology on IMD[J]. Aeronautical Computer Technique, 2004, 34(1): 119-121.

[14] 张 文. 针对 ARP 和 PPPoE 的攻击与检测技术研究[D]. 成都: 四川师范大学, 2013.

[15] 侯功华, 赵远东. 基于 NDIS 中间层的包过滤的研究与设计[J]. 微计算机信息, 2006, 22(12-3): 141-143.