广西科学院学报
Journal of Guangxi Academy of Sciences

2009,25(3):216~218
Vol. 25,No. 3 August 2009

ARP 欺骗攻击类型及防御方案
Type and Defense Solution of ARP Spoofing Attack

苏宏庆,梁正安
SU Hong-qing,LIANG Zheng-an

(广西计算中心,广西南宁 530022)
(Computing Center of Guangxi, Nanning,Guangxi,530022,China)

摘要:分析 ARP 原理以及欺骗网关攻击、仿冒网关攻击、"中间人"攻击和泛洪攻击 4 种常见的 ARP 欺骗攻击类型,结合电子政务网 ARP 防御的应用实例,提出一种采用 DHCP 服务器和交换机的 DHCP Relay Agent、DHCP Snooping 功能进行防御 ARP 欺骗攻击的方案。该方案能够防止接入终端任何 ARP 欺骗攻击,可以有效解决 ARP 欺骗攻击问题。

关键词:ARP 攻击 防御 网络安全
中图法分类号:TP393 **文献标识码**:A **文章编号**:1002-7378(2009)03-0216-03

Abstract: The principle of ARP and four kinds of common types of ARP attack including deceiving gateway attack, phishing gateway attack, "middleman" attack and flooding attack were introduced and analyzed. By combining with an application of defensing ARP attack in E-government network, a solution for ARP spoofing attack by using DHCP server, DHCP Relay Agent and DHCP Snooping function of switch was proposed. This solution can prevent all ARP spoofing attack of access terminal, which effectively resolve the problem of ARP spoofing attack.

Key words: ARP,attack,defense, network security

随着互联网的发展,网络应用日益广泛,网络病毒和攻击的形式多样化,危害和规模越来越大,网络安全已经成为一个突出的问题。近期大规模爆发的 ARP 病毒和 ARP 攻击就是一个典型的代表。ARP 是地址解析协议,是一种将 IP 地址转化成物理地址(MAC 地址)的协议[1]。ARP 具体来说就是将 OSI 的第 3 层网络层地址(32 位 IP 地址)解析为 OSI 的第 2 层数据连接层的 MAC 地址。ARP 欺骗攻击针对 ARP 协议设计固有的缺陷,采用发送假 ARP 报文的方式欺骗和攻击目标。ARP 欺骗攻击不同于其它病毒,它的攻击是基于基础网络协议的天然缺陷,其核心就是破坏网络设备的 ARP 表,使得设备无法查到 IP 地址对应的正确 MAC 地址,导致报文发送错误,网络通信瘫痪。ARP 欺骗攻击不仅攻击 PC 机,还攻击路由器、交换机等各种网络设备,传播和危害范围很广[1]。因此,ARP 欺骗攻击攻击的防御不同于常见病毒,单靠传统杀毒软件和防火墙难以根除。ARP 欺骗攻击既可能造成网络内出现随机断线,也可能造成整个网络瘫痪,还可能造成通信被窃听、信息被篡改等各种严重后果。本文在介绍分析 ARP 原理和常见的 ARP 欺骗攻击类型的基础上,提出网络中 ARP 欺骗攻击的一种防御方案。

1 ARP 原理及 ARP 欺骗攻击类型

1.1 ARP 原理分析

ARP 协议是属于链路层的协议,在以太网中的数据帧从一个主机到达网内的另一台主机是根据 48 位的以太网地址(硬件地址)来确定接口,而不是根据 32 位的 IP 地址[1]。ARP 原理为:A 要向主机 B 发送报文,会查询本地的 ARP 缓存表,找到 B 的 IP 地址对应的 MAC 地址后,就会根据 MAC 地址进行数据传输。如果未找到,则主机 A 广播一个 ARP 请求报文,报文携带 A 的 IP 地址 IP-a,A 的物理地址 MAC-a,目标主机 B 的 IP 地址 IP-b,目标 MAC 地址为 FF-FF-FF-FF(ARP 广播报文目标 MAC 地址

收稿日期:2009-07-03
作者简介:苏宏庆(1980-),男,助理工程师,主要从事计算机应用和网络安全研究。

为全"1"),请求 IP 地址为 IP-b 的主机 B 回答物理地址 MAC-b。网上所有主机包括 B 都收到 ARP 请求,但只有主机 B 识别自己的 IP 地址,于是向主机 A 发回一个 ARP 响应报文,其中就包含有主机 B 的 MAC 地址。主机 A 接收到主机 B 的应答后,就会更新本地的 ARP 缓存,在 ARP 表中加入主机 B 的 IP 地址到 MAC 地址映射的 ARP 表项。接着使用这个 MAC 地址发送数据(由网卡附加 MAC 地址)。本地高速缓存的 ARP 表是本地网络数据转发的基础,而且这个缓存是动态的。

1.2 ARP 欺骗攻击类型

ARP 协议并不只是在发送了 ARP 请求才接收 ARP 应答。当计算机接收到 ARP 应答数据包的时候,就会对本地的 ARP 缓存进行更新,将应答中的 IP 和 MAC 地址存储在 ARP 缓存中。ARP 协议是基于网络中的所有主机或者网关都为可信任的前提制定,在 ARP 协议中没有认证的机制,从而导致针对 ARP 协议的欺骗攻击非常容易。ARP 欺骗是黑客常用的攻击手段之一,常见的 ARP 欺骗有欺骗网关攻击、仿冒网关攻击、"中间人"攻击和泛洪攻击 4 种 ARP 攻击类型。

1.2.1 欺骗网关攻击

欺骗网关攻击的现象为网络中部分 PC 机掉线,甚至全网内 PC 机都无法上网。查看路由器的 ARP 表项,发现很多错误地址,所有被攻击者的 IP 地址对应的 MAC 地址都为攻击者的 MAC 地址。重启路由器后恢复正常,但是过一段时间 PC 又开始掉线。

欺骗网关攻击是攻击者通过伪造 ARP 报文,发送源 IP 地址为同网段内某台合法用户的 IP 地址,源 MAC 地址为伪造的 MAC 地址的 ARP 报文给网关,使网关更新自己的 ARP 表中原合法用户的 IP 地址与 MAC 地址的对应关系。网关发送给原合法用户的所有数据全部重定向到一个错误的 MAC 地址(攻击者),导致该用户无法正常与网关通信。

1.2.2 仿冒网关攻击

仿冒网关攻击的现象表现为,在同一局域网中,有一部分 PC 机被攻击无法上网。重启被攻击的 PC 机后恢复正常,但是过一段时间后网络又中断。查看每台无法上网的 PC 机(被攻击 PC)的 ARP 表,发现网关的 MAC 地址错误。被攻击 PC 机的 ARP 表中的网关 192.168.1.1 的 MAC 地址已被修改成另一台 PC 机(攻击者)的 MAC 地址,被攻击 PC 机无法再同网关通信,无法上网。

仿冒网关攻击是攻击者通过伪造 ARP 报文,发送源 IP 地址为网关 IP 地址,源 MAC 地址为伪造的 MAC 地址的 ARP 报文给被攻击的主机,使这些主机更新自己的 ARP 表中网关 IP 地址与 MAC 地址的对应关系。主机访问网关的流量,被重定向到一个错误的 MAC 地址,导致该用户无法正常与网关通信。

1.2.3 "中间人"攻击

"中间人"攻击又称为 ARP 双向欺骗[2]。"中间人"攻击的现象主要表现为:网络中某台 PC 上网突然掉线,一会又恢复了但是恢复后一直上网很慢,查看该 PC 机的 ARP 表,网关 MAC 地址已被修改,而且网关上该 PC 机的 MAC 地址也是伪造的。该 PC 机和网关之间的所有流量都转到另外一台机子上。

如果有恶意攻击者(Host B)想探听 Host A 和网关之间的通信,它可以分别给 Host A 和网关发送伪造的 ARP 应答报文,使 Host A 和网关用 MAC-B 更新自己的 ARP 映射表中与对方 IP 地址相应的表现。此后,Host A 和网关之间看似"直接"的通信,实际上都是通过黑客所在的 HostB 间接进行的,即 Host B 担当了"中间人"的角色,可以对信息进行了窃取和篡改。

1.2.4 泛洪攻击

泛洪攻击的现象表现为:网络经常中断,或者网速很慢,查看 ARP 表项也都正确,但是在网络中抓包分析,发现大量的 ARP 请求报文。

泛洪攻击是恶意用户利用工具构造大量的 ARP 报文发往交换机、路由器或某台 PC 机,导致 CPU 忙于处理 ARP 协议,负担过重,造成设备没有资源转发正常的数据流量。

2 ARP 欺骗攻击的防御方案

我们以某市电子政务网的 ARP 防御方案为例,提出网络中 ARP 欺骗攻击的一种防御方案。

某市电子政务网网络的结构分 3 层结构:由核心层、汇聚层和接入层组成。接入层由四大班子部门及其他政府委办局单位组成,通过千兆光纤,以星型方式连接到汇聚层,各单位划分独立的接入单位(VLAN)。应用服务器群直接接到核心层交换机。某市电子政务网网络拓扑图如图 1 所示。

我们对整个网络采用 DHCP 服务器和交换机的 DHCP Relay Agent、DHCP Snooping 功能[3]从接入层进行 ARP 欺骗攻击防御。实施方案主要分为 3 个部分。

第一，在服务器群区塔建一台DHCP服务器，在DHCP服务器上为每个VLAN创建一个域，分配不同的IP地址段、子网掩码、网关和DNS等参数。

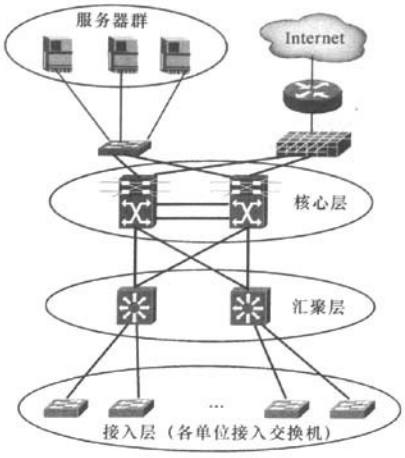

图1 某市电子政务网拓扑结构

——：100M以太网；——：1000M光纤

第二，由于各接入单位的DHCP客户机与DHCP服务器（位于服务器群区）不在同一个网段，需要在交换机上启用DCHP Relay Agent（中继代理）。用DHCP Relay代理可以去掉在每个网段都要有DHCP服务器的必要，它可以传递消息到不在同一个子网的DHCP服务器，也可以将服务器的消息传回给不在同一个子网的DHCP客户机。其工作原理为：(1)当DHCP客户机启动并请求DHCP初始化时，它会在本地网络广播配置请求报文。(2)如果本地网络存在DHCP服务器，则服务器可以直接对DHCP客户机进行DHCP配置，不需要DHCP Relay。(3)如果本地网络没有DHCP服务器，则与本地网络相连的具有DHCP Relay功能的网络设备收到该广播报文后，将进行适当处理并转发给指定的其它网络上的DHCP服务器。(4)DHCP服务器根据DHCP客户机提供的信息进行相应的配置，并通过DHCP Relay将配置信息发送给DHCP客户机，完成对DHCP客户机的动态配置。

第三，在接入层交换机部署ARP入侵检测，接入交换机启用DHCP Snooping对DHCP报文进行监测。DHCP Snooping监控用户动态申请IP地址的全过程，通过监测DHCP报文记录用户的IP/MAC/VLAN/PORT等信息，并形成一个DHCP Snooping绑定表。交换机端口接收到的ARP报文后，识别并读取ARP报文内容，通过查找DHCP Snooping建立的绑定关系表，来判断ARP应答报文的发送者源IP、源MAC是否合法。如果ARP报文中的发送者源MAC、IP匹配绑定表中的内容，则认为是合法的报文，交换机转发该报文；如果ARP报文中的发送者源MAC、IP与绑定表中的内容不匹配，则认为是欺骗攻击报文，交换机对ARP欺骗报文进行丢弃处理。ARP泛洪攻击经常伴随着发送大量的ARP报文，消耗网络带宽资源和交换机CPU资源，造成网络丢包率高，网速降低，甚至全网瘫痪。针对ARP泛洪攻击的这一特点，在接入交换机上部署ARP报文限速，对每个端口单位时间内接收到的ARP报文设置阀值，当端口在单位时间内ARP报文超过阀值时直接关闭该端口，并设置默认恢复时间，恢复时间为相对时间30s，即端口在自动关闭30s后重新打开。以上的配置可以很好地保障了网络带宽资源和交换机CPU资源，从而有效防范ARP泛洪攻击。交换机ARP入侵检测能够防止接入终端发起任何ARP欺骗攻击，可以有效解决ARP欺骗攻击问题。

3 结束语

本文介绍分析ARP协议的原理及4种常见的ARP欺骗攻击类型，并结合某电子政务网ARP防御的应用实例，提出一种ARP欺骗攻击的防御方案。该方案在接入层部署ARP安全防御，能有效的阻止攻击数据包转发到汇聚层和核心层交换机，保护了交换机的资源，保证网络的高效运行；同时采用DHCP服务器动态给客户机分配IP地址，降低了网管人员的维护工作量。该方案具有实施部署简单，无需在终端配置参数，防范效率高等特点，能够有效解决ARP欺骗攻击问题。

参考文献：

[1] Jeff Doyle. Routing TCP/IP: Valume I [M]. Indianapolis: Macmillan Technical Publishing, 1998.

[2] 曾梦良，郑雪峰. 基于接入层的网络安全解决方案研究[J]. 微计算机信息，2007，10(3)：72-74.

[3] Craig Hunt, Robert Bruce Thompson. Windows NT TCP/IP 网络管理[M]. 王颖，译. 北京：中国电力出版社，2000.

（责任编辑：韦廷宗）