跨网段 ARP 欺骗的原理及防治策略的研究

单家凌

(广东白云学院 计算机系,广东 广州 510450)

摘 要: ARP 协议主要实现了网络层地址到数据链路层地址的动态映射,由于 ARP 协议具有无序性、无确认性、动态性、无安全机制等特性,ARP 欺骗攻击成了局域网中一种常见的攻击现象。在深入研究 ICMP 重新定向原理的基础上,通过一个实例解释了跨网段 ARP 欺骗原理和具体实现过程,并给出了具体的检测与防范方法。

关键词: ARP;重新定向;ICMP;跨网段

中图分类号: TP393.08 **文献标识码**: A **文章编号**: 1674-7720(2010)21-0069-03

Inter-network segment ARP spoofing principle and research of control strategies

SHAN Jia Ling

(Department of Computer, Guangdong Baiyun Institute, Guangzhou 510450, China)

Abstract: ARP protocol mainly implements dynamic mapping from network-layer's address to datalink-layer's address. However, it has many characteristics like no sequence, no confirmation, dynamism, no safe mechanism. ARP spoofing attack has become a common phenomenon attacks in LAN. This paper studied the principle of ICMP redirection, explained inter-network segment ARP spoofing principle and the realization process, and gave the specific method of detection and prevention.

Key words: ARP; redirection; ICMP; inter-network segment

网络安全是当今网络技术的一个重要研究课题,有很强的现实应用背景。在网络安全防范中,地址解析协议 ARP(Address Resolution Protocol)是一个相当重要的内容,也是网络攻击者最偏向于利用的网络底层协议。ARP 协议的设计是建立在局域网内计算机互信的基础上的,这种设计的初衷使得今天局域网内出现了大量的与 ARP 相关的木马和病毒,严重影响了局域网内通信的安全和通信效率,给用户利益带来了巨大的风险。研究 ARP 攻击的原理与欺骗的防御方法,有助于加强局域网的安全建设,提高局域网内各主机的通信安全和网络的性能。本文针对跨网段的 ARP 攻击进行了研究。

1 ARP 协议

1.1 ARP 的作用

ARP[1]工作在数据链路层,在本层与硬件接口联系,同时对上层(网络层)提供服务。在以太网中,由于以太网设备并不识别 32 bit 的 IP 地址,所以数据包的传送不是通过 IP 地址完成的,而是通过 48 bit MAC 地址(网卡的物理地址)来完成的,一台主机要和另一台主机进行直接通信,必须要知道目标主机的 MAC 地址。而 ARP 协议用于将网络中的 IP 地址解析为 MAC 地址,以保证通信的顺利进行。ARP 工作时,首先请求主机发送出一个含有所希望到达的 IP 地址的以太网广播数据包,然后目标 IP 的所有者会以一个含有 IP 和 MAC 地址对的数据包应答请求主机。这样请求主机就能获得要到达的 IP 地址对应的 MAC 地址,同时请求主机将这个地址对放入自己的 ARP 表缓存起来,以节约不必要的 ARP 通信。主机每隔一段时间(或者当收到 ARP 应答)都会用新的地址映射记录对 ARP 缓存进行更新,以保证自己拥有最新的地址解析缓存。ARP 的报文格式如表 1 所示[2]。

表 1 ARP 报文格式

硬件类型		协议类型
硬件地址长度	协议长度	操作
发送方硬件地址(8 bit 组 0~3)		
发送方硬件地址(8 bit 组 4~5)		发送方 IP 地址(8 bit 组 0~1)
发送方 IP 地址(8 bit 组 2~3)		目标硬件地址(8 bit 组 0~1)
目标硬件地址(8 bit 组 2~5)		
目标 IP 地址(8 bit 组 0~3)		

1.2 ARP 协议的安全问题

ARP 协议是建立在信任局域网内所有结点的基础上的,它高效,但却不安全。ARP 高速缓存根据所接收到的 ARP 协议包随时进行动态更新,它是无状态的协议,不会检查自己是否发过请求包,只要收到目标 MAC 是自己的 ARP 响应数据包或 ARP 广播包(包括 ARP 请求数据包和 ARP 响应数据包),都会接受并缓存。ARP 协议没有认证机制,只要接收到的协议包是有效的,主机就无条件地根据协议包的内容刷新本机 ARP 缓存,并不检查该协议包的合法性。因此攻击者可以随时发送虚假 ARP 包更新被攻击主机上的 ARP 缓存,进行地址欺骗或拒绝服务攻击。

2 跨网段的 ARP 需重新定向的原因

如果是同一网段,ARP 欺骗攻击就可以直接通过洪水攻击或伪造 IP-MAC 地址映射表来实现,但是如果伪造包是经过路由分段将无法获得成功,因为即使使用洪水攻击或者伪造包使得目标主机无法提供服务,失去连接,局域网中的主机也只是在局域网中找目标主机而根本不会与攻击主机通信,因为主机路由表到目标主机的路由是直接交付而不是经过网关交付,这时需要再伪造一个网际控制报文协议 ICMP(Internet Control Message Protocol)重定向报文广播包,通知目标主机所在的局域网中的所有主机:到达目标主机的最短路径不是直接交付,而是路由,需要重定向。这样所有主机在接收重定向报文后更新自己的路由表,攻击主机就可以伪装成目标主机进行通信。

3 ARP 与 ICMP 跨网段重定向

3.1 ICMP 重定向报文格式

ICMP 是为了更有效地转发 IP 数据报和提高交付成功的机会。它在主机和路由器之间报告差错情况和提供异常情况的报告,目的是为了当网络出现问题的时候返回控制信息。ICMP 重定向报文是 ICMP 差错报告中的一种请求改变路由的报文。表 2 为 ICMP 重定向报文格式[3]。

重定向报文的类型为 5,代码有效值为 0~3。其中 0 代表网络重定向,1 代表主机重定向,2 代表服务类型和网络重定向,3 代表服务类型和主机重定向。原则上,重定向报文是由路由器产生而供主机使用的。路由器默认发送的重定向报文也只是 1 或者 3,只是对主机的重定向,而不是对网络的重定向。而主机本身不是路由器,所以这种 ICMP 重定向会导致网络流量的增大。

表 2 ICMP 重新定向报文格式

Byte 0	Byte 1	Byte 2	Byte 3
类型	代码	校验和	
重定向网关 IP			
原包的 IP 首部			
源 IP 数据报前 8 个字节			

3.2 ICMP 重定向报文程序

ICMP 重新定向所使用的报文程序如下:

```
//ICMP header
typedef struct _tagX_icmphdr{
unsigned char i_type;                                    //类型
unsigned char i_code;                                    //代码
unsigned short i_cksum;                                  //检验和
unsigned short i_id;                                     //标识符
unsigned short i_seq;                                    //序列号
unsigned long i_timestamp;
  //当前时间 itmestump=(unsigned long);GetTickCount();
XIcmpHeader;
case ICMP-REDIRECT:
  if (code>3)
   goto badcode;
  if (icmplen < ICMP-ADVLENMIN ||icmplen <ICMP-ADVLEN (icp))
   ||icp->icmp-ip·ip-hl<(sizeof(struct ip)>>2))
  {
  icmpstat.icps-badlen++;
    break;
  }
  icmpgw·sin-addr=ip->ip-src;
  icmpdst·sin-addr=icp->icmp-gwaddr,
  icmpsrc·sin-addr=icp->icmp-ip·ip-dst;
  rtredirect ((struct sockaddr*) &icmpsrc,
  (struct sockaddr*) &icmpdst,
  (struct sockaddr*) 0, RTF-GATEWAY|
  RTF-HOST,(struct sockaddr*)&icmpgw,
  (struct rtentry**) 0);
  ptctlinput (PRC-REDIRECT-HOST,(struct sockaddr*)&icmpsrc);
   Break;
```

3.3 ICMP 重定向的工作原理

在 Internet 网的主机发送数据报时,先查找自己的路由表,判断发送接口。出于效率的考虑,主机并不和连接在网络上的路由器定期交换路由信息,一般在主机中

设置一个默认路由器的IP地址，数据报先传送给这个默认路由器，此默认路由器通过与其他路由器交换路由信息得知到达每一个网络的最佳路由，当默认路由器发现主机发往某个目的地址的数据报的最佳路由不是本默认路由器而是另一个路由器时，就用改变路由报文把这种情况告诉主机，主机即更改路由表增加一个新路由项目。

下面用如图1所示的实例来说明ICMP重新定向的过程。主机PC要ping路由器RB的f1地址：192.168.2.1/24，主机将判断出目标属于不同的网段，因此它要将ICMP请求包发往自己的默认网关192.168.0.253/24(路由器RA的f0接口)。但是，这之前主机PC首先必须发送ARP请求，请求路由器RA的f0(192.168.1.253/24)的MAC地址。当路由器RA收到此ARP请求包后，首先用ARP应答包回答主机PC的ARP请求(通知主机PC：路由器RA自己的f0接口的MAC地址为AA-AA-AA-AA)。然后，路由器RA将此ICMP请求转发到路由器RB的f0接口：192.168.0.254/24（要求路由器RA正确配置了到网络192.168.2.0/24的路由)。此外，路由器RA还要发送一个ICMP重定向消息给主机PC，通知主机PC对于主机PC请求的地址的网关是：192.168.0.254。路由器RB此时会发送一个ARP请求消息请求主机PC的MAC地址，而主机PC会发送ARP应答消息给路由器RB。最后，路由器RB通过获得的主机PC的MAC地址信息，将ICMP应答消息发送给主机PC。

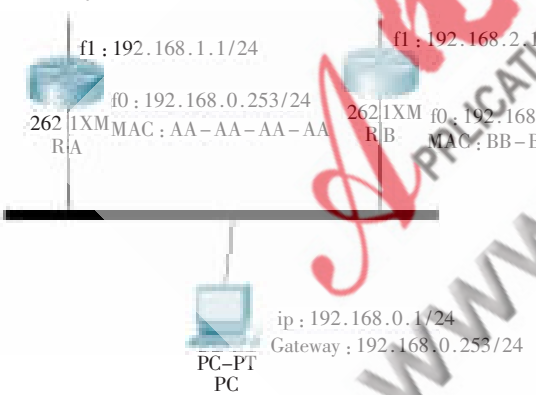

图1 ICMP重新定向

3.4 跨网段的ARP欺骗攻击的实现过程

跨网段的ARP欺骗比同一网段的ARP欺骗要复杂得多，它需要把ARP欺骗与ICMP重定向攻击结合在一起。假设A和B在同一网段，C在另一网段，如表3所示。

表3 跨网段主机IP地址和MAC地址对应表

主机	IP地址	MAC地址
A	192.168.0.1	AA-AA-AA-AA
B	192.168.0.2	BB-BB-BB-BB
C	192.168.2.1	CC-CC-CC-CC

首先攻击方C修改IP包的生存时间，将其延长，以便做充足的广播。然后和上面提到的一样，寻找主机B的漏洞，攻击此漏洞，使主机B暂时无法工作。此后，攻击方C发送IP地址为B的IP地址192.168.0.2，MAC地址为C的MAC地址CC-CC-CC-CC的ARP应答给A。A接收到应答后，更新其ARP缓存。这样，在主机A上，B的IP地址就对应C的MAC地址。但是，A在发数据包给B时，仍然会在局域网内寻找192.168.0.2的MAC地址，不会把包发给路由器，这时就需要进行ICMP重定向，告诉主机A到192.168.0.2的最短路径不是局域网，而是路由，请主机重定向路由路径，把所有到192.168.0.2的包发给路由器。主机A在接收到这个合理的ICMP重定向后，修改自己的路由路径，把对192.168.0.2的数据包都发给路由器。这样攻击方C就能得到来自内部网段的数据包。

4 ARP病毒的检测和防范策略

4.1 ARP的检测方法[4]

(1)主动定位方式。因为所有的ARP病毒攻击源都会有其特征——网卡会处于混杂模式，可以通过ARPKiller工具扫描网内有哪台机器的网卡是处于混杂模式的，从而判断这台机器有可能就是攻击机。定位好机器后，再做病毒信息收集，提交给相关单位做分析处理。

(2)在任意客户机上进入命令提示符(或MS-DOS方式)，用arp-a命令查看。如果看到有两个机器的MAC地址相同，那么就可以判断网络内有ARP欺骗攻击。

(3)运行tracert -d网址。如果第一个跳显示的不是网关而是其他的IP地址，则第一跳中显示的IP即为中了ARP病毒计算机的IP地址。

4.2 ARP欺骗的安全防范策略[5]

(1)编写一个批处理文件arp.bat，实现开机运行，将交换机网关的MAC地址和网关的IP地址绑定，内容如下：

```
@echo off
arp-d
arp-s IP MAC
```

其中IP和MAC为网关IP地址和MAC地址。

(2)网管交换机端绑定。在核心交换机上绑定用户主机的IP地址和网卡的MAC地址，同时在边缘交换机上将用户计算机网卡的MAC地址和交换机端口绑定的双重安全绑定方式。

以思科2950交换机为例，输入命令：

```
Switch#config terminal # 进入配置模式
Switch(config)# Interface f 0/1
# 进入具体端口配置模式
Switch(config-if)switchport
port-security mac-address MAC(主机的MAC地址)
```

(3)算法的实现[6]。根据ARP欺骗过程，防止ARP欺

骗可以基于这样的思想：如果ARP响应报文是在发出ARP请求之后收到的，则接收该响应，并更新ARP缓存。如果接收到ARP响应报文不是在发送ARP请求之后，则拒绝该响应。该算法的具体实现过程中，设置一个数组ReqAddBuf[i]，保存陆续发出的 n 个ARP请求包的目的IP地址，均赋初值0。设置两个参数：ReqEntryIP和ResEntryIP，分别保存当前发出的ARP请求报文的目的IP地址和接收到的ARP响应报文的源IP地址。设置两个逻辑变量 *Sendin-gReqPack* 和 *ReceivingResPack*。首先，察看是否在发送ARP请求报文，如果正在发送，就将该IP加入到数组ReqAddBuf[i]中。C语言描述如下：

```
if (SendingReqPack= =1)
{ for (i=1; i<=n ; i++)
 { if (ReqAddBuf[i] = = 0)
  {ReqAddBuf[i] = ReqEntryIp;
   break;}
   else if (i= =n)
      {n = n+1;
       i = n;
       ReqAddBuf[i] = ReqEntryIp; }
 }
}
```

当接收到一个ARP响应报文时，察看它的源IP地址是否记录在案，如果有，则更新ARP高速缓存；如果没有，丢弃该响应报文。C语言描述如下：

```
if (ReceivingResPack= =1)
{ for (i=1; i<=n ; i++)
 {if (ReqAddBuf[i]= = ResEntryIP)
  { ReqAddBuf[i]=0;
   UpdateArp( );
   break;}
   else if (i= =n) DelResPack();
  }
}
```

该方案可以通过修改TCP/IP内核源代码(主要是修改广播ARP请求函数 *arprequest* 和处理接收到的ARP报文的函数 *in_arpinput*)得以实现；也可以做一个软件，在每次发送和接收ARP报文时进行相应处理。

(4)使用ARP服务器。ARP服务器保存有局域网内各主机的IP地址和MAC地址的映射信息，并且禁用局域网内除服务器之外各主机的ARP应答，仅保留服务器对接收到的ARP请求进行应答。但是必须要保证ARP服务器的正常运行，不被黑客攻击。

(5)使用防火墙等安全产品。现在大多网络公司在防火墙等安全产品中加入了对ARP欺骗的防范，它们通常是从底层驱动对所有ARP欺骗数据包进行识别和屏蔽，使ARP欺骗攻击无功而返。

依据ICMP的重新定向，ARP欺骗攻击可以跨网段进行，这样就扩大了ARP进行攻击的范围，这对于ARP欺骗的防御又增添了难度。由于ARP本身的设计问题，使得要彻底避免ARP欺骗攻击几乎不可能。因此，除了做好防范以外，经常查看当前的网络状态，对网络活动进行分析、监控，采取积极、主动的防御行动是保证网络的安全和畅通的重要和有效的方法。

参考文献

[1] 除晨.ARP欺骗防御研究[D].保定：河北农业大学，2009.
[2] 姜晓峰.ARP协议简析与ARP欺骗攻击防范[J].电脑知识与技术，2008(1)：1349-1350
[3] 佚名.ICMP重定向差错. http://www.77169.com/classical/HTML/51616.html，2010-06-01.
[4] 范俊俊.基于交换机的ARP安全机制研究[J].计算机工程与设计，2008(8)：4162-4164
[5] 金涛.公众网络环境中的ARP欺骗攻击与防范方法[D].上海：上海交通大学，2007.
[6] 徐功文.ARP协议攻击原理及其防范措施[J].网络与信息安全，2005(1)：4-6.

(收稿日期：2010-07-03)

作者简介：

单家凌，男，1979年生，硕士，主要研究方向：网络安全。