文章编号：1000－1573(2009)03－0125－05

一种基于报文过滤防御ARP欺骗的系统架构①

陈 晨， 韩宪忠， 王克俭
（河北农业大学 信息科学与技术学院，河北 保定 071001）

摘要：本研究分析了ARP欺骗的基本原理及其常见的攻击方式；讨论了现有防御方法存在的局限性。在此基础上，提出了一种防御ARP欺骗的构想，并设计和开发了一套基于C/S模式的ARP防御系统软件。该系统以局域网内每台主机都有唯一的IP地址与MAC地址相对应为基础，通过在客户端对接收到的ARP报文进行ARP报文头信息检验和服务器端IP－MAC检验，过滤掉存在安全隐患的报文，来实现局域网内主机对ARP欺骗的防御，从而提高网络安全性。该系统适用于安全性较高的中小型局域网络。

关 键 词：ARP欺骗；TCP/IP；C/S模式；报文过滤；网络安全
中图分类号：TB 393.08 文献标识码：A

A system architecture against ARP spoofing based on packet filtering

CHEN Chen, HAN Xian-zhong, WANG Ke-jian
(College of Information Science and Technology, Agricultural University of Hebei, Baoding 071001, China)

Abstract: This paper analyses the basic theory of ARP spoofing and some common attacking methods of ARP spoofing. The paper also discusses three preventive methods against ARP spoofing and their limitations. According to the analyses, an approach to designing a client-server model software is put forward in order to resist ARP spoofing. The system is based on the relative that every host in LAN has a unique IP address to its MAC address. The client detects header of all ARP packets that host receives and abandons the ARP packets of inconsistent－header. The server examines the authenticity of IP address and MAC address of source host in ARP packets from the client, then makes the client filter out the unsafe packets. Through this process, the system can effectively prevent local computer from ARP spoofing, and improve network security. The system is applicable to small and medium－sized local area networks, which need higher security requirements.

Key words: ARP spoofing; TCP/IP; C/S model; packet filtering; network security

ARP协议全名为Address Resolution Protocol（地址解析协议），是一个TCP/IP协议，工作在网络层与数据链路层之间，用于局域网中根据目标主机的IP地址来获得其MAC地址[1]。ARP欺骗利用了ARP协议自身设计上的缺陷来达到监听、窃取用户数据资料、破坏网络正常运行环境的目的。ARP欺骗的突出表现为局域网内主机经常掉线，重启交换机后恢复正常，但数分钟后又开始掉线。针对愈演愈烈的ARP欺骗，研究ARP协议的漏洞并设计一个防御ARP欺骗的方法来加强局域网内主机安

① 收稿日期：2008－10－20
作者简介：陈 晨（1983－），男，河北保定人，在读硕士生，研究方向：计算机网络与数据库.
通讯作者：韩宪忠（1965－），男，河北泊头人，教授，主要从事网络与数据库方面的研究.

全的工作显得十分必要。

1 ARP 欺骗的原理及攻击方式分析

ARP 协议是建立在网络中各主机相互信任的基础上的[2]，虽然实现了简单、高效的传输，但是存在着安全隐患。ARP 协议是无状态协议，不会检测自己是否发过请求包，也不检测是否是合法的应答，只要收到 ARP 应答包或 ARP 广播，就会接受并更新 ARP 缓存。

ARP 欺骗的核心思想就是向目标主机发送一个伪造了源 IP－MAC 映射的 ARP 应答，使目标主机收到该应答帧后更新其 ARP 缓存，从而使目标主机将报文发送给错误的对象[3]。如图 1 所示[4]，利用 ARP 欺骗，攻击者借助主机 B 使 A 在毫无察觉的情况下将原本要发送至 C 的报文发送至 D。

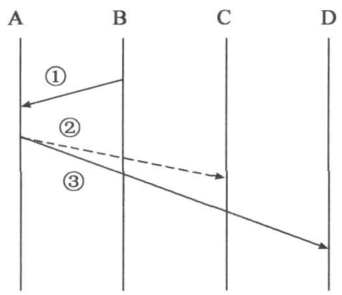

图 1 ARP 欺骗原理

Fig. 1 Theory of ARP spoofing

其中 D 为任意主机；①B 向 A 发送 ARP 应答(请求)报文，将 C 的 MAC 地址映射为 D；②A 正在(或准备)向 C 发送报文；③A 接收到 B 发送的 ARP 欺骗报文后将报文发给 D。

通过对 ARP 协议漏洞及攻击原理的分析，总结出 ARP 欺骗攻击方式有以下几方面：

(1)发送伪造的 ARP 请求报文。攻击者发送一个修改了源 IP 地址和 MAC 地址的请求报文，使局域网其它接收此报文的主机更新 ARP 缓存，来实现欺骗目的。

(2)发送伪造的 ARP 应答报文。目前大多数操作系统对应答报文，一旦接收立即更新其 ARP 缓存，并不进行是否发出过 ARP 请求的验证；即使主机曾经发送过 ARP 请求报文并接收到真实的应答报文，也会因后到的伪造应答而再次更新 ARP 缓存。因此，直接伪造应答报文即可实现欺骗。

(3)发送伪造的免费 ARP(gratuitous ARP)请求和应答报文。伪造免费 ARP 请求和应答报文可使局域网内任意 1 台主机产生 IP 地址冲突错误。广播免费 ARP 请求还可以使其他接收报文主机更新 ARP 缓存。

2 ARP 欺骗的常见解决方案及其局限性

(1)添加静态的 ARP 缓存记录[5]。在 ARP 缓存中设置静态的 IP－MAC 地址的映射，即使主机接收到伪造的 ARP 应答也不会刷新缓存，从而防止 ARP 欺骗的发生。但此方法是手工操作，适用于小型的局域网，且对部分操作系统(如 Windows2000)无效。

(2)采用交换机端口绑定[6]。交换机的每个端口与主机 MAC 地址都一一绑定，一旦连接主机 MAC 地址发生变化则锁定此端口，将主机排除于局域网外。此方法可以阻止攻击者发送伪造报文，但遇到主机位置发生变化等问题，仍需要人工重新绑定交换机各端口，且大多数局域网使用低端交换机，并不具备绑定功能。

(3)修改 ARP 协议。Bruschi[7] 引入非对称加密机制，提出一种 S－ARP 协议来替换 ARP 协议。而 Lootah[8] 采用另一种基于非对称加密机制的 T－ARP 协议。Goyal[9] 使用数字签名技术和基于 hash 链表的一次一密方案结合，提高了协议实施效率。修改 ARP 协议的方法从根本上解决了 ARP 协议存在的缺陷，但 ARP 协议的广泛使用使得修改 ARP 协议这种方法的推广需要付出巨大的代价。

以上 3 种方法虽然可以解决或部分解决 ARP 欺骗问题，但是其自身的应用实施都存在着较大的不足。因此，研究一种新的防范 ARP 欺骗方法就显得十分重要。

3 一种防御 ARP 欺骗系统的设计架构

针对主机接收 ARP 报文并更新 ARP 表中 IP-MAC 对应信息时不检验更新内容的可靠性的缺陷，设计一套基于 C/S 模式的 ARP 欺骗防御软件。该系统软件以局域网内每台主机都具有唯一的 IP-MAC 对应作为基础，它包括 2 部分：服务器端和客户端。指定局域网中某台计算机为服务器，并安装服务器端软件，其他主机安装客户端软件。客户端负责依照规则对本机接收到的 ARP 报文进行检测，发现非法报文则抛弃并报警；服务器端保存有网内所有主机的 IP－MAC 映射信息，并检验客户端提交的 IP-MAC 对应信息是否与服务器端保存映射相

一致，将结果返回客户端。

3.1　服务器端

服务器端保存局域网内所有的 IP－MAC 映射信息，主要作用是对客户端提交的 IP－MAC 映射数据进行检验，并告知客户端检验结果。它包括数据库、IP－MAC 列表维护模块和与客户端交互模块 3 部分。数据库是数据存储中心，保存局域网内所有主机的 IP－MAC 映射记录；IP－MAC 列表维护模块提供添加、修改、删除已有映射记录的功能；与客户端交互模块负责与客户端进行交互、提供 IP－MAC 映射数据检验结果。如图 2 所示：

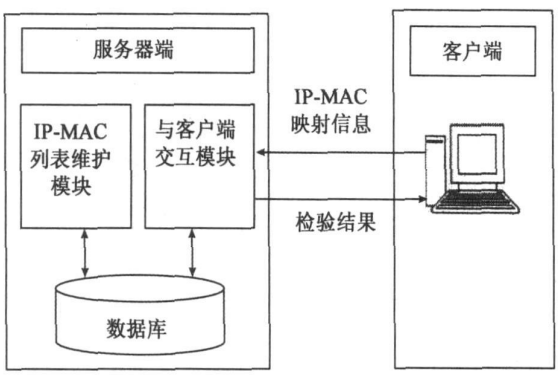

图 2　服务器端与客户端交互图

Fig 2　Communication between server and client

3.2　客户端

客户端是主机防范 ARP 欺骗的关键，对接收到的 ARP 报文进行检验并处理，主要由 ARP 报文头信息检验和 ARP 报文过滤两部分组成。根据 ARP 欺骗的攻击方式，可以看出主机接收 ARP 请求报文事件和接收 ARP 应答报文事件都能使主机更新 ARP 缓存。所以，ARP 报文头信息检验和 ARP 报文过滤就需要针对这两种事件做出必要处理。

3.2.1　ARP 报文头信息检验　在以太网中，ARP 报文封装成为以太网数据帧传送，并在数据帧头中保存有源主机的地址信息。如图 3 所示。

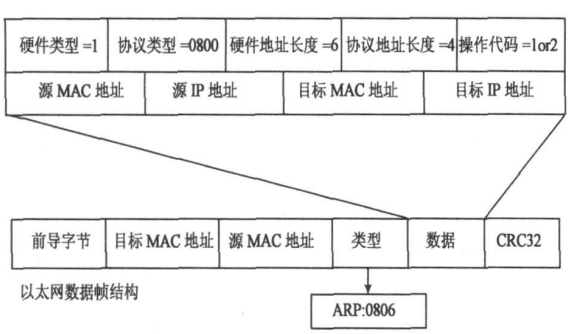

图 3　以太网 ARP 协议报文结构

Fig. 3　ARP packet structure and frame structure

在正常状态下，ARP 报文中源主机 MAC 地址与目标 MAC 地址应该和以太网数据帧头中的源主机 MAC 地址与目标 MAC 地址相一致。通过网络捕获包采样研究发现，攻击者总是伪造 ARP 报文，修改报文中的源主机地址信息以达到逃避追踪的目的。经过这种方式处理过的 ARP 报文，其报文中包含的 MAC 地址信息是不同于以太网数据帧头中的 MAC 地址信息，应该抛弃。以下给出客户端 ARP 报文头信息检验算法：

```
(1)ARP 请求报文头信息检验部分
if(ARP 请求报文)
{  /*帧头源 MAC 地址 Eth_Mac_Src 和报文源 MAC 地址 Arp_Mac_Src 是否一致 */
   if(Eth_Mac_Src ! =Arp_Mac_Src)
   {  放弃报文，报警；}
}
(2)ARP 应答报文头信息检验部分
if(ARP 应答报文)
{  /*帧头源 MAC 地址 Eth_Mac_Src 和目标 MAC 地址 Eth_Mac_Dst 与报文源 MAC 地址 Arp_Mac_Src 和目标 MAC 地址 Arp_Mac_Dst 是否分别一致 */
   if(Eth_Mac_Src ! =Arp_Mac_Src||Eth_Mac_Dst ! =Arp_Mac_Dst)
   {  放弃报文，报警；}
}
```

3.2.2　ARP 报文过滤　经过 ARP 报文头信息检验的报文，并不能说明其来源就是安全的，仍然需要去除掉其中并未在服务器端注册的 IP－MAC 映射信息的报文，以保证更新 ARP 缓存信息内容的可靠性。

为客户端设计一个线性表 ArpList，用于保存通过服务器端检验的 IP－MAC 映射记录。此表的主要目的是避免多次向服务器端查询相同 IP 报文，减轻网络负载。ArpList 表初始加载服务器主机的 IP－MAC 映射记录。客户端收到 ARP 报文后，取出 ARP 报文中 IP 和 MAC 地址，以 IP 方式查找 ArpList 表中是否存在相应记录。如果存在记录则更新 ARP 缓存；不存在则连接服务器进行 IP－MAC 映射信息验证。如果返回验证结果为正确，将报文中源 IP 和 MAC 地址记录加入 ArpList 表并更新 ARP 缓存，如果返回验证结果错误则抛弃报文。给出 ARP 报文过滤算法：

```
(1)ARP 请求报文过滤部分
if(ARP 请求报文)
```

```
{   if(调用 ARP 请求报文头信息检验不通过)
    {   放弃报文,报警; return;}
    /*报文目标 IP 地址 Arp_Ip_Dst 是否是本地 IP 地址 Ip_Local */
    if(Arp_Ip_Dst==Ip_Local)
    {   if(ArpList 表含有源 IP 地址 Arp_Ip_Src 的映射记录)
        {   if(报文源 IP 地址 Arp_Ip_Src 和 MAC 地址 Arp_Mac_Src 与记录不一致)
            {   放弃报文,报警; return;}
            发送应答报文,更新 ARP 缓存;
        }
        else
        {连接服务器,发送 Arp_Ip_Src 和 Arp_Mac_Src 信息,并获取验证结果;
            if(验证结果为不正确)
            {   放弃报文,报警; return;}
            将 Arp_Ip_Src 和 Arp_Mac_Src 映射信息加入 ArpList 表;
            发送应答报文,更新 ARP 缓存;
        }
    }
    /*免费 ARP 请求报文处理,即报文目标 IP 地址 Arp_Ip_Dst 与源 IP 地址 Arp_Ip_Src 相等 */
    else if(Arp_Ip_Dst==Arp_Ip_Src)
    {/*与处理 ARP 请求报文过程基本相同,但不发送应答报文 */
        ……
    }
}
```

(2)ARP 应答报文过滤部分

```
if(ARP 应答报文)
{   if(调用 ARP 应答报文头信息检验不通过)
    {   放弃报文,报警; return;}
    if(ArpList 表含有报文中源 IP 地址 Arp_Ip_Src 的映射记录)
    {if(报文源 IP 地址 Arp_Ip_Src 和 MAC 地址 Arp_Mac_Src 与记录不一致)
        {   放弃报文,报警; return;}
        更新 ARP 缓存;
    }
    else
    {连接服务器,发送 Arp_Ip_Src 和 Arp_Mac_Src 信息,并获取验证结果;
        if(验证结果为不正确)
        {   放弃报文,报警; return;}
        将 Arp_Ip_Src 和 Arp_Mac_Src 映射信息加入 ArpList 表;
        更新 ARP 缓存;
    }
}
```

4 系统实现及结果测试

在 Windows 系统中,利用 Winsock 技术实现客户端与服务器端通信,NDIS 中间层[10](Intermediate Driver,MD)技术实现客户端对接收到的 ARP 报文进行检验与处理。NDIS 中间层驱动位于网卡驱动程序与协议驱动程序之间,所有从网络接收到的数据均需从此经过。因此,采用中间层技术可以过滤掉从网络接收到的不安全的 ARP 报文。依照前述的 ARP 报文头信息检验和报文过滤的方法,系统对所有拦截的 ARP 数据包进行处理,对每个接收的 ARP 报文进行检测,可以使主机有效地过滤掉伪造的 ARP 报文。

表 1 主机 IP—MAC 对应表

Table 1 IP—MAC Mapping Table

主机类型 Sorts of main computer	IP	MAC
服务器	192.168.0.1	00—0D—87—C6—2E—4F
攻击主机	192.168.0.100	00—0D—87—CF—34—56
目标主机	192.168.0.101	00—0D—87—BD—2D—9E
辅助主机	192.168.0.102	00—0D—87—CC—87—3A

在 Windows 系统中实现此系统,并在 100 M 带宽的局域网中进行测试。测试主机 4 台,配置为 P4 2.6G,512M 内存主机,其中一台为服务器,并已保存有全部测试主机的 IP—MAC 对应信息;另外 3 台分别为攻击主机、目标主机、辅助主机,目标主机安装有客户端,如表 1 所示。攻击主机使用 WinArpAttacker3.5 分别发送伪造的 ARP 请求报文和 ARP 应答报文;目标主机显示报警信息,ARP 缓存表并未被伪造报文篡改,如表 2 所示。由于加入了网络通信验证和线性表结构,增加了主机的资源消耗,但不影响系统正常运行。

表 2　测试结果表
Table 2　Test result table

攻击主机 Attacking computer							目标主机 Object computer
发送 ARP 报文类型	目标硬件 MAC	源硬件 MAC	目标协议 MAC	目标 IP	源协议 MAC	源 IP	ARP 缓存表
Request	00－0D－87－BD－2D－9E	00－00－00－00－00－00	00－0D－87－BD－2D－9E	192.168.0.101	AA－AA－AA－AA－AA－AA	192.168.0.100	192.168.0.100 伪造映射不存在
Request	00－0D－87－BD－2D－9E	00－0D－87－CF－34－56	00－00－00－00－00－00	192.168.0.101	00－0D－87－CF－34－56	192.168.0.102	192.168.0.102 伪造映射不存在
Reply	00－0D－87－BD－2D－9E	00－0D－87－CF－34－56	00－0D－87－BD－2D－9E	192.168.0.101	00－0D－87－CF－34－56	192.168.0.102	192.168.0.102 伪造映射不存在

5　总结

ARP 欺骗利用了 ARP 协议的缺陷,为局域网内计算机用户带来了极大的危害。本文通过分析 ARP 欺骗的原理,探讨了 3 种防御 ARP 欺骗的解决方案及其局限性,提出了一种新的 ARP 欺骗防御系统架构。该系统基于 C/S 模式设计,结合客户端接收到的 ARP 报文头信息检验及在服务器端 IP－MAC 检验,有效防御 ARP 欺骗攻击,提高局域网内主机通信的安全性。由于系统会带来部分网络性能及主机资源损耗,适用于安全性要求较高的中小型局域网,如网吧、学校机房、办公小型局域网等。

参考文献:

[1] RICHARD STEVENSW. TCP/IP 详解(卷 1:协议)[M]. 北京:机械工业出版社, 2000.

[2] 张洁, 武装, 陆倜. 一种改进的 ARP 协议欺骗检测方法[J]. 计算机科学, 2008, 35(3):52－54.

[3] SEAN WHALEN. An Introduction to ARP Sp－oofing [EB]. http://packetstormsecurity.org/papers/protocols/index.html, 2001.

[4] 郑文兵, 李成忠. ARP 欺骗原理及一种防范算法[J]. 江南大学学报, 2003, 2(6):574－577.

[5] 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, 182.

[6] 林宏刚, 陈麟. 一种主动检测和防范 ARP 攻击的算法研究[J]. 四川大学学报, 2008, 40(3):143－149.

[7] Bruschi D, Ornaghi A, Rosti E. S－ARP: A secure address resolution protocol[C] //Proceedings of the 19th Annual Computer Security Applications Conference. NV, USA: IEEE computer Society, 2003.

[8] Lootah W, Enck W, McDaniel P. TARP ticket-based address resolution protocol[C] //Computer Security Applications Conference ACSAC 2005, 21st Annual. Tucson, Arizona, USA: IEEE computer Society, 2005.

[9] Goyal V, Tripathy R. An efficient solut－eion to the ARP cache poisoning problem[C] //10th Australasian Conference on In formation Security and Privacy (ACISP2005). LNCS3574, Germany: Springer－Verlag, 2005.

[10] 范莉萍. 基于 NDIS 技术的个人防火墙设计与实现[J]. 计算机应用与软件, 2008, 25(8):259－260.

(编辑:张月清)