基于ARP协议的局域网访问控制

刘贵松，晏 华，章 毅

(电子科技大学计算机科学与工程学院 成都 610054)

【摘要】提出了一种基于地址解析协议(ARP)的局域网访问控制方案。通过实时捕获、分析了网络数据报发现登录局域网络的非法主机，采用ARP协议机制杜绝其对局域网内合法主机的非法访问；利用服务器对网络主机IP地址、MAC地址和其他辅助信息的多重认证，以及网络主机客户端ARP缓存机制实现网内合法主机之间的限制访问，从而有效地保护局域网资源。

关 键 词 局域网; 地址解析协议; 访问控制; 资源保护

中图分类号 TP309 文献标识码 A

The Access Control of Local Area Network Based on ARP Protocol

LIU Gui-song，YAN Hua，ZHANG Yi

(School of Computer Science and Engineering, UEST of China Chengdu 610054)

Abstract The access control of local area network is a common security problem which involved the resource protection of local area network. In this paper, a project of access control of local area network based on ARP protocol is presented. It can be used to detect and refuse the illegal computers that try to log on and access the local area network by capturing and analyzing the network packets. On the other hand, through the authentication of the local area network server and based on the ARP buffer principle, it can be also used to control the access between the legal computers of the local area network. So that it is an effective way to protect the resource of local area network. The project is convenient and useful.

Key words local area network; address resolution protocol; access control; resource protection

计算机网络安全是各国国家与国防安全的重要组成部分，也是各国国家信息化建设与发展的关键。因此，计算机网络安全是一个国际化的问题。目前，我国各企事业单位的局域网络数不胜数。从网络安全的角度看，各企事业单位内部系统被外部入侵、破坏及泄密是一个严重问题，而来自于内部入侵的安全问题更应引起人们的重视。通过简便可行的技术手段并辅之以科学的管理，可以使对局域网络的访问得到控制，从而杜绝非法主机访问。本文提出一种基于地址解析协议(Address Resolution Protocol，ARP)机制的局域网访问控制方案，较好地实现了局域网资源的保护和访问控制。

1 基于ARP机制的局域网访问控制方案的物理模型

通常，企事业单位构筑的局域网都是基于TCP/IP协议的星型以太网络。每个单位都设有多个部门，各部门具有自己的业务系统以及部门内部的共享资源，通过集线器或者交换机连接，如图1所示。

基于ARP机制的局域网访问控制方案所要解决的关键问题是：1) 如何探测外来非法机器登录局域网络并采取相应措施杜绝其访问；2) 如何通过灵活的权限设定限制局域网内合法机之间的非授权互访。

收稿日期：2003 – 11 – 10

作者简介：刘贵松(1973 –)，男，在职博士生，讲师，主要从事神经网络、信息安全方面的研究.

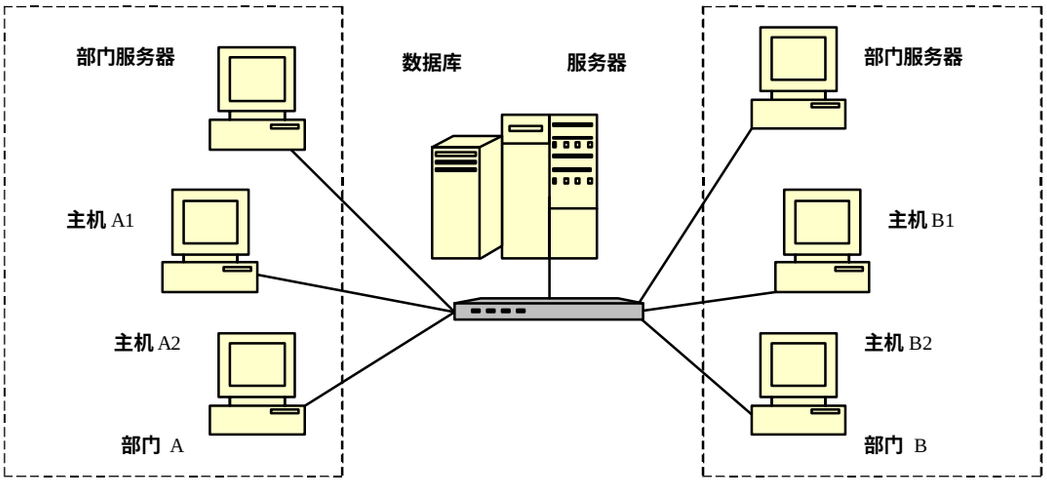

图1　普通局域网网络拓扑图

2　ARP以及ARP高速缓存表

2.1　ARP协议

TCP/IP协议是一组完整的网络协议，ARP是网络层中的一个重要协议。在局域网中，当一台主机把以太网数据帧发送到另一台主机时，是根据48 bit以太网地址来确定目的接口的。网络中实际传输的每一帧里包含有目标主机的介质访问控制子层(Media Access Control，MAC)地址。在以太网中，一个主机要和另一个主机进行直接通信，必须要知道目标主机的MAC地址。而MAC地址可以通过地址解析协议获得。所谓“地址解析”就是在IP地址和采用不同网络技术的硬件地址之间提供的动态映射。将MAC地址转换为网络地址是通过反向地址解析协议(Reverse Address Resolution Protocol, RARP)来实现的。由此可见，ARP的基本功能就是通过目标主机的IP地址，查询其物理MAC地址，以保证通信的顺利进行。

2.2　ARP缓存表

网络上每台主机都有一个ARP缓存表，这也是ARP高效运行的关键所在。缓存表中存放了最近的Internet地址到硬件地址之间的映射记录。可以通过[arp –a]命令查看本机ARP缓存内容。以主机A向主机B发送数据为例，当发送数据时，主机A会在本机的ARP缓存表中寻找是否有目标IP地址。如寻找到，将目标主机MAC地址写入以太网帧首部加入到输出队列等候发送；否则，主机A就会在网络上发送一个ARP请求广播，询问同一网段内主机B的MAC地址。网络上其他主机并不响应该ARP询问，只有主机B的ARP层收到这份报文后，才会向主机A发送一个ARP应答，告知其MAC地址为“00-E0-4C-87-DD-D2”，如表1所示。

表1　IP/MAC地址对应表

主机	IP地址	MAC地址
A	192.168.0.1	00-10-AB-1F-0C-61
B	192.168.0.2	00-E0-4C-87-DD-D2
C	192.168.0.3	00-AB-D3-6C-89-E3

由此，主机A获得主机B的MAC地址，可以向主机B发送信息。同时更新本机的ARP缓存表，以便下次再向主机B发送信息时，直接从ARP缓存表里查找。

每台初次登录网络的机器在建立网络连接时，都要发送ARP广播包；在本机ARP缓存表中如果不存在即将访问主机的IP/MAC地址，也将向网络发送ARP请求。由此可以根据每个用户的既定访问权限信息对主机的ARP缓存表作相应改变，从而达到访问控制的目的。

2.3　ARP缓存老化机制

按照缺省设置，ARP高速缓存中的项目是动态的，每当发送一个指定地点的数据报且高速缓存中不存在当前项目时，ARP便会自动添加当前项目。ARP缓存采用老化机制，在一段时间内如果表中的某一行没有被使用，该行就会被删除，如此可以大大缩小ARP缓存表的长度，加快查询速度。因此，访问控制要求所

进行的ARP缓存改变必须进行定时刷新，从而适应ARP缓存老化机制。

3 网络监听

3.1 网络监听原理

在网络中，当信息进行传播的时候，通过某种方式将其截获或者捕获，从而进行分析处理，称之为网络监听。网络监听在网络中的任何一个位置模式下都可实施。

1) 信息发送。Ethernet网协议的工作方式是将要发送的数据报发往连接在一起的所有主机。包头中包括有应该接收数据报的主机的正确地址。要发送的数据报必须从TCP/IP协议的IP层交给数据链路层，在这个过程中，采用ARP将网络地址翻译成48 bit的MAC地址。

2) 信息接收。Ethernet中填写了物理地址的帧经网卡发送到物理线路上。当使用集线器的时候，发送出去的信号到达集线器，由集线器再转发到相连接的每一条线路。当数字信号到达一台主机的网络接口时，正常状态下，网络接口对读入数据帧进行检查，决定是否将数据帧交给IP层软件。但是，当主机工作在监听模式下时，所有的数据帧都将被交给上层协议软件处理。以太网卡典型地具有一个“混合模式(Promiscuous)”选项，能够关掉过滤功能而查看经过它的所有数据报。这个混合模式选项恰好被数据报监测程序利用来实现它们的监听功能。

3.2 分析数据报

在网络监听时，常常要保存大量的信息，并对收集的信息进行大量的分析和处理。因此，监听和数据分析如果不加协议过滤，由此带来的系统开销不容忽视。同时，如果分析过程不加缓存，许多包就会来不及接收而被漏走。所以监听程序通常将已经捕获到的数据报进行缓存然后分析，二者之间的延迟要视具体的应用进行设置。

基于ARP机制的局域网访问控制方案中，由于所关注的焦点是访问者的身份验证以及访问者的权限和控制，因此，监听和分析的数据报类型可以设定为ARP请求/响应数据报，不仅可以达到对非法登录局域网主机的探测，而且大大减少了监听的容量以及分析处理的时间。

4 设计与实现

参考图1，结合企事业单位的实际运行环境考虑软件功能设计和最终部署，可以将整个局域网结构分为中心认证服务器(Certification Authority_Server)、部门服务器(Dept_Server)和各部门客户机(Client)三层，具体系统设计规划可分为五个部分，程序名称、功能以及部署位置如下：1) 主机管理(Host_Manager)，部署于局域网服务器端，负责整个局域网内的主机管理、注册、认证；2) 网络监测(CA_Monitor)，部署于局域网服务器端，监听非法主机登录、对非法主机发送欺骗信息；3) 部门管理(Dept_Manager)，部署于局域网部门服务器端，实现部门主机管理、访问控制权限设置；4) 主机注册(Host_Register)，部署于局域网客户端，实现合法主机注册、登录认证；5) 缓存刷新(Write_ARP)，部署于局域网客户端，获取权限信息、更新ARP缓存。

4.1 局域网合法主机注册

局域网内合法主机定义为单位内部且通过CA_Server注册的主机。对一台合法主机通过由网络管理员分配的网内IP地址、本机网卡MAC地址和本机其他相关的系统信息(如CPU的ID号码、硬磁盘信息等)进行唯一识别。

通过IP地址和MAC地址的绑定验证，基本可以确定主机的网络身份，同时辅之验证系统信息，即可杜绝IP地址盗用、MAC地址修改等一系列安全隐患。

在网络通讯正常时，Host_Manager程序为每台合法主机生成一个加密的注册文件，Host_Register启动后根据注册文件信息进行注册，并获得本机其他系统信息，发送至CA_Server进行注册。注册通过后的每一次启动都将进行登录认证。如认证不合法，系统自动进行锁定，等待网络管理员进行处理。

4.2 合法主机间访问控制

4.2.1 访问控制权限设置

通过Dept_Manager可以设置本部门主机的访问权限。系统缺省为全部可以访问，可以依据实际情况设

置拒绝访问主机列表。每台主机的访问权限根据授权情况实时保存于CA_Server后台数据库中。根据通信双方约定的惯例，拒绝访问可以单方面实施，而要求申请访问则必须得到对方确认。

4.2.2　更改客户端ARP缓存

Write_ARP程序安装后以系统进程的方式在后台运行。主机启动后首先通过SOCKET方式从认证服务器取得本机的访问权限列表；系统将拒绝访问主机的IP地址以及构造的虚假MAC地址{0x00, 0x1A, 0x2B, 0x3C, 0x4D, 0x5F}相对应，并实时写入本机ARP高速缓存表中。写ARP缓存每条信息之间的时间间隔设为10 ms。由前述分析可知，为了保证权限设定生效的实时性以及适应ARP缓存表的老化机制，程序设计中采用多线程方式。

4.3　非法主机登录监听及处理

CA_Monitor程序实现网络ARP请求/应答数据报的监测和分析。

4.3.1　截获、分析数据报

数据报截获程序调用WinPcap2.7版本驱动程序，支持Win32平台上的信息包捕获和网络分析。具体实现时可直接调用驱动程序的应用编程接口(API)。

通过AnalyzeArpPack(Char * Buffer)过程分析捕获的ARP数据报，得到源主机IP地址以及MAC地址，然后通过系统已经注册的合法主机信息，判断当前发送ARP请求的主机是否合法。

图2为系统监测到非法主机以IP 192.168.0.157登录的情况。

图2　CA监视器运行图

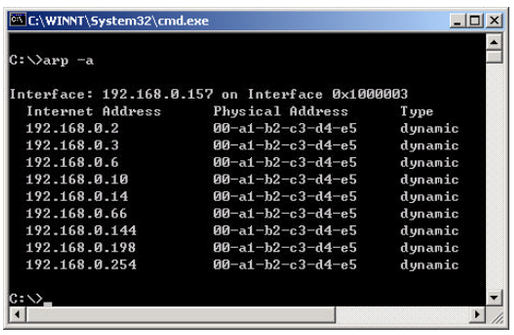

图3　非法主机ARP缓存结果图

4.3.2　发送ARP欺骗信息

通过数据报截获分析，系统探测到非法主机登录网络或者试图访问，系统将根据合法主机IP信息，构造虚假MAC地址，使用特定线程对非法主机进行持续欺骗。根据实际运行情况，考虑到网络负担以及系统性能，欺骗信息连续发送时间可为2～5 min，每轮间隔为10～20 s。系统运行所得结果如图3。

5　结 束 语

通过对实际应用网络模型的分析，利用ARP协议机制以及网络主机ARP高速缓存表机制，提出了一种局域网访问控制方案，并设计和实现了相应的软件系统。该软件系统在实际运行过程中稳定可靠，耗用主机资源少，较好实现了基于局域网络的资源保护。

参 考 文 献

[1] Stevens W R. TCP/IP详解 卷1: 协议[M]. 北京: 机械工业出版社, 2000

[2] Stevens W R. TCP/IP详解 卷2: 实现[M]. 北京: 机械工业出版社, 2000

[3] Socolofsky T, Kale C. RFC1180 A TCP/IP Tutorial[DB/OL]. www.sino2000.com.cn, 2003-10-08

[4] 易发胜, 彭　孜, 李成林. Windows网络体系结构分析及网卡驱动程序设计[J]. 计算机应用, 1999, 10(1): 61-63

[5] 朱颖靓, 王　晓, 李　婷. 基于Windows平台的网络封包截获技术研究[J]. 青岛大学学报, 2003, 16(2): 156-160

编　辑　熊思亮