ARP 欺骗的监测与防范技术综述 *

秦丰林[1]，段海新[2]，郭汝廷[1]
（1. 山东大学 网络中心，济南 250100；2. 清华大学 网络工程研究中心，北京 100084）

摘　要：目前已经提出许多针对 ARP 欺骗的安全技术，根据所起作用的不同，将其分为 ARP 欺骗监测、ARP 欺骗防御和改进 ARP 协议的 ARP 欺骗避免技术。主要对这些技术进行分析和总结，比较其优缺点，并提出研究改进 ARP 协议需要综合考虑的因素。

关键词：ARP 协议；ARP 欺骗；ARP 欺骗监测；ARP 欺骗防御；ARP 欺骗避免
中图分类号：TP309　　**文献标志码**：A　　**文章编号**：1001-3695(2009)01-0030-04

Overview of ARP spoofing detection and prevention techniques

QIN Feng-lin[1], DUAN Hai-xin[2], GUO Ru-ting[1]
(1. *Network Center, Shandong University, Jinan* 250100, *China*; 2. *Network Engineering Research Center, Tsinghua University, Beijing* 100084, *China*)

Abstract: Up to now, many schemes have been proposed to protect against ARP spoofing which can be classified into three categories as detecting, preventing and avoiding techniques according to their functions. This paper summarized and analyzed each of these schemes, identified their advantages and weaknesses, presented some factors that have to be considered in improving ARP protocol.

Key words: ARP protocol; ARP spoofing; ARP spoofing detection; ARP spoofing prevention; ARP spoofing avoidance

ARP 欺骗具有隐蔽性、随机性的特点，在 Internet 上随处可下载的 ARP 欺骗工具[1,2]使 ARP 欺骗更加普遍。攻击者可以利用 ARP 欺骗进行拒绝服务攻击（DoS）或中间人攻击，造成网络通信中断或数据被截取和窜改，严重影响网络的安全。目前利用 ARP 欺骗的木马病毒在局域网中广泛传播，给网络安全运行带来巨大隐患，是局域网安全的首要威胁[3]。如何有效地监测和防范 ARP 欺骗攻击成为当前网络管理者所面临的严峻挑战。由于 ARP 欺骗问题的严重性，研究者已经提出许多针对 ARP 欺骗的安全防范技术。

1　ARP 欺骗原理

ARP 协议[4]即地址解析协议（address resolution protocol），是网络层中的一个重要协议。地址解析是指在 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。在以太网中，当一台主机 Y 想与另外一台主机 X 通信时，需要获取主机 X 的 MAC 地址，获取流程如图 1 所示。Y 首先检查 ARP 缓存表中是否有 X 的 MAC，如果没有就会向局域网广播 ARP 请求“谁是 x. x. x. x，请告诉 MAC yy-yy-yy-yy-yy-yy”，局域网内的所有主机都会收到这个 ARP 请求，但是只有主机 X 才会响应这个请求，它会回应一个单播的 ARP 应答包“我是 x. x. x. x，MAC 是 xx-xx-xx-xx-xx-xx”。这样，主机 Y 就把 X 的〈IP，MAC〉地址映射保存在 ARP 缓存表中，之后主机 Y 与 X 之间的通信就依靠两者缓存表中的 MAC 地址，直到这个〈IP，MAC〉地址映射超时（缺省 ARP 超时时间如表 1 所示），才重新发起 ARP 解析请求。

表 1　缺省 ARP 超时时间

操作系统	ARP 超时时间/min	操作系统	ARP 超时时间/min
Windows 2000/XP	2	Linux	1
Free BSD	20	Solaris	5

ARP 协议是建立在信任局域网内所有节点的基础上，虽然高效却并不安全。ARP 协议是一种无状态的协议，它不会检查自己是否发过请求报文，也不管（其实也不知道）是否是合法应答，只要接收到目标 MAC 是自己的 ARP 广播报文，都会接收并更新缓存，这就为 ARP 欺骗提供了可能。

ARP 欺骗是指局域网内的恶意节点发送伪造的 ARP 报文以更新其他节点的 ARP 缓存表，来达到影响网络通信的目的[5]。由于局域网内的每台主机内都存有 ARP 缓存表，ARP 攻击者将发送大量的 ARP 欺骗报文以淹没正常的 ARP 报文，使得主机的 ARP 缓存表内记录假的 MAC 信息，从而达到 ARP 欺骗的目的。根据被欺骗对象的不同，ARP 欺骗可以分为欺骗主机、欺骗网关、双向欺骗三种类型。文献[6]中详细介绍攻击者可以利用 ARP 欺骗进行 DoS 攻击、MAC 伪装、中间人攻击（图 2）等攻击类型，在局域网中造成网络通信异常、敏感数据泄露、数据被窜改、网页劫持、非法控制等严重后果。

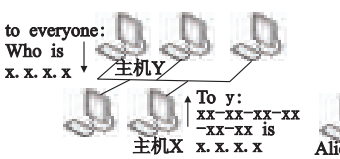

图1　ARP协议工作流程

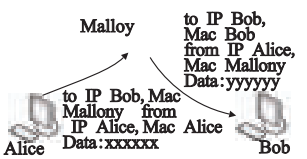

图2　利用ARP欺骗进行中间人攻击

收稿日期：2008-04-22；**修回日期**：2008-07-09　　**基金项目**：山东省自然科学基金资助项目（Y2007G42）

作者简介：秦丰林（1978-），男，山东潍坊人，工程师，博士研究生，主要研究方向为计算机网络技术与多媒体通信（qfl@sdu.edu.cn）；段海新（1972-），男，副教授，博士，主要研究方向为计算机网络安全与管理；郭汝廷（1965-），男，工程师，硕士，主要研究方向为计算机网络应用与管理.

2　ARP 欺骗监测与防御技术

2.1　ARP 欺骗监测技术

1)手动监测　文献[7]详细介绍了手动监测 ARP 欺骗所采用的方法。网络管理员可以通过命令查看主机的 ARP 表或路由器 ARP 表,也可以利用 Ethereal[8] 等 Sniffer 工具进行抓包,发现可疑的〈IP, MAC〉地址映射,分析可能存在的 ARP 欺骗并判断欺骗类型。图 3 是利用命令查看路由器 ARP 表时发现有多个 IP 地址对应一个 MAC 的现象,这就说明该局域网内存在欺骗网关类型的 ARP 欺骗。

Internet	202.194.8.105	0	Incomplete	ARPA
Internet	202.194.8.145	0	00e0.fc07.31be	ARPA
Internet	202.194.8.147	–	00e0.fc07.31be	ARPA
Internet	202.194.8.152	0	00e0.fc07.31be	ARPA
Internet	202.194.8.154	1	00e0.fc07.31be	ARPA
Internet	202.194.8.155	1	00e0.fc07.31be	ARPA
Internet	202.194.8.156	1	00e0.fc07.31be	ARPA
Internet	202.194.8.157	0	Incomplete	ARPA
Internet	202.194.8.170	1	00e0.fc07.31be	ARPA

图3　查看路由器ARP表发现ARP欺骗

2)动态监测　它可以分为被动监测和主动监测两种。例如 ARPWatch[9] 和 ARP-Guard[10] 属于被动监测,仅监测网络中是否存在 ARP 欺骗,并不主动向外发送 ARP 报文;ARP 防火墙则属于主动监测,在监测网络是否存在 ARP 欺骗的同时,还主动向外发送 ARP 报文,防止对本机进行 ARP 欺骗。

ARPWatch 是一个在局域网内监听 ARP 报文的专用工具。在监测到〈IP,MAC〉地址映射出现可疑的改变时,通过邮件通知网络管理员。ARPWatch 轻便有效,特别适用于小规模网络。入侵监测系统 Snort[11] 也具有与 ARPWatch 相类似的 ARP 欺骗监测功能,但它主要是一个安全预警软件,ARP 欺骗监测只是其中一小部分功能,应用具有局限性。

ARP-Guard 采用了一种基于 SNMP 探针的分布式监测架构,通过对网络监听和 SNMP 探针取得的信息分别进行动态分析,以判断网络中是否有 ARP 欺骗并及时通知网络管理员。与 ARPWatch 相比,ARP-Guard 增加了 SNMP 探针模块,可以应用于大规模网络。但 ARP-Guard 是一款商业软件,不能免费使用。

ARP 防火墙是一种安装在用户主机上的 ARP 欺骗监测软件[12],能够动态监测局域网内针对本主机和针对网关的 ARP 欺骗。但是如果设置错误,主动监测的 ARP 防火墙会向局域网内发送大量 ARP 报文,造成 ARP 报文的广播风暴,影响网络通信。因此 ARP 防火墙的应用具有两面性。

2.2　ARP 欺骗防御技术

1)手动防御　防御 ARP 欺骗的简单方法是网络管理员分别在主机和路由器上静态绑定〈IP, MAC〉地址映射。这种方法非常有效,但仅适用于小规模的局域网。随着网络规模的扩大,即使有相关软件协助进行〈IP,MAC〉地址映射的绑定[13],手动添加的方法也会使工作量迅速增加。而且这种方法不适用于 DHCP 自动分配地址的情况,也不能适应网络的动态变化。

另一种有效的手动防御方法是在局域网中增加 VLAN 的数目,减少 VLAN 中的主机数量。这种方法能够缩小 ARP 欺骗影响的网络范围;缺点同样是增加了网络维护的复杂度,也无法自动适应网络的动态变化。

2)动态防御　MAC 伪装是 ARP 欺骗的一个变种[6]。Port-Security[14] 是思科交换机支持的一种防御 MAC 伪装的技术。使能 Port-Security 的交换机端口只允许学习有限数量的 MAC 地址,如果设置为 1,则只允许一个合法的主机连接网络,伪装的 MAC 地址就无法通过交换机。这种方式对防御 MAC 伪装非常有效,但不能解决其他类型的 ARP 欺骗问题。

文献[15 ~ 17]分别利用 Shell 脚本、Winpcap 开发库、SNMP 协议等实现了一种针对 ARP 欺骗的动态监测防御系统,在监测到发生 ARP 欺骗后,及时采取措施定位 ARP 欺骗主机,并关闭其连接,避免 ARP 欺骗的扩散。其工作原理基本一致,如下所述:

a)ARP 欺骗监测。根据不同类型的 ARP 欺骗的表现特征,分别采取端口镜像监听网络、报文分析、分析路由器日志和分析路由器 ARP 表等方法,动态发现网络中可能存在的 ARP 欺骗。另外,文献[16]还采用了一种将采集到的〈IP,MAC〉地址映射与数据库中保存的记录相比较的方法,如果不相符则认为存在 ARP 欺骗。这种方法需要收集局域网内所有主机的 IP 和 MAC 地址,这也由该软件自动采集完成,克服了手动防御中需要手动绑定〈IP, MAC〉地址映射的缺点。

b)ARP 欺骗主机定位。在监测到 ARP 欺骗后,首先需要确定发起 ARP 欺骗主机的 MAC 地址,然后对连接该主机的交换机设备定位;最后再对连接该主机的交换机端口进行定位,定位操作主要通过 SNMP 协议完成。

c)关闭该主机连接。在完成主机和交换机端口定位后,利用 SNMP 协议关闭连接该主机的交换机端口,并以邮件或网页的形式通知用户。

动态的监测与防御系统可以根据 ARP 欺骗类型分别采取相应的监测方法,对发起 ARP 欺骗的主机及时定位并断开连接,准确率较高,能够有效地避免 ARP 欺骗的扩散,在一定程度上缓解了局域网内 ARP 欺骗的问题。但是该系统只是在监测到 ARP 欺骗之后进行处理,不能从根本上解决 ARP 欺骗的问题。另外,局域网中大规模爆发的 ARP 欺骗在系统监测到问题前就已经使网络不能正常通信,影响系统的监测效果,只能由网络管理员参与处理。

3　ARP 欺骗避免技术

ARP 欺骗是由于 ARP 协议的安全缺陷以及信任局域网内主机造成的。要彻底避免发生 ARP 欺骗,必须对 ARP 协议进行改进,增强其安全特性。为与上面总结的 ARP 欺骗防御技术相区别,本文称之为 ARP 欺骗避免技术。

3.1　中间件技术

Tripunitara 等人[5] 提出一种利用中间件(middleware)技术来监测与抵御 ARP 欺骗的方法。其主要思想是在系统内核中增加一个 checker 模块,它位于网卡驱动与上层驱动之间,负责监测流入和流出的 ARP 报文并进行处理,如图 4 所示。

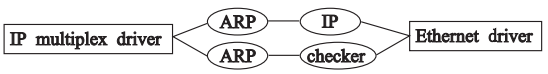

图 4　中间件技术修改的内核结构

修改的系统内核对 ARP 报文的处理流程如下:

a)在发送 ARP 请求报文时,checker 添加该请求到 ARP 请求报文列表。

b)在接收 ARP 应答报文时, checker 首先检查请求报文

列表中是否存在对应的 ARP 请求。若存在则进行转发，并添加到 ARP 应答报文列表；若不存在，再检查 ARP 应答报文列表中是否有对应的 ARP 应答记录，若有则进行转发，否则丢弃。

中间件技术的优点是修改系统内核的主机，可以有效地监测和防御 ARP 欺骗，并与局域网中其他内核未作改变的主机相兼容；缺点是需要修改系统内核，而且没有考虑防止本机对其他主机发起 ARP 欺骗。一种改进的方法是修改系统内核发送 ARP 报文的处理策略。在系统内核发送 ARP 请求或应答报文时，checker 首先检查 ARP 报文的合法性，如果 ARP 报文的源地址是本机的 MAC 地址，则进行转发；否则丢弃。

Anticap[18] 与中间件技术相类似，也需要修改系统内核，它是 UNIX 类型系统的一个内核补丁。Anticap 在监测到 ARP 报文中的〈IP，MAC〉地址映射与系统 ARP 缓存表不一致时，拒绝更新 ARP 缓存表，并记录到系统日志中供以后参考。这种方法增加了 ARP 欺骗的难度，但不适用于采用 DHCP 动态分配 IP 地址的情况，具有局限性。

3.2　加密与认证技术

ARP 协议建立在信任局域网内主机的基础上，对 ARP 报文不作任何加密和认证，这是 ARP 欺骗产生的重要原因。文献[19～22]分别提出利用加密认证技术来改进 ARP 协议，通过对 ARP 报文进行认证避免发生 ARP 欺骗。

Gouda 等人[19] 提出一种新的地址解析架构，它包括一个安全服务器和两种新协议：邀请—接受和请求—应答。邀请—接受协议用于主机向安全服务器注册其〈IP，MAC〉地址映射；请求—应答协议用于主机向安全服务器请求局域网中其他主机的 MAC 地址。这种架构与标准的 ARP 协议不兼容，且安全服务器存在单点故障问题。但是它为利用安全认证技术改进 ARP 协议提供了很好的借鉴。

安全 ARP 协议（S-ARP）是由 Brushi 等人[20] 于 2003 年提出的一种 ARP 协议改进方案。其主要思想是利用非对称加密技术来对 ARP 报文进行认证，避免发生 ARP 欺骗。安全 ARP 协议需要在局域网中增加一个权威密钥分发服务器（authoritative key distributor，AKD），用来保存局域网中每台主机的 IP 地址和公钥。运行安全 ARP 协议的主机需要连接到 AKD 服务器获取发送 ARP 报文主机的公钥，对接收到的 ARP 报文进行验证，同时主机缓存该公钥以提高运行效率。安全 ARP 协议只需在标准 ARP 报文的尾部增加一个认证字段用于携带发送主机的数字签名，因此与 ARP 协议相兼容。安全 ARP 协议的优点是利用非对称加密技术验证 ARP 报文的合法性，与 ARP 协议相兼容，但仍存在 AKD 服务器单点故障和重放攻击等缺点，而且安全 ARP 协议存在的认证过程影响了运行效率。文献[21]基于安全 ARP 协议的架构提出一种改进方案，采用将数字签名与基于哈希链的一次性密码技术相结合的方法来验证 ARP 报文，提高安全 ARP 协议的运行效率。

票据 ARP 协议（ticket-ARP）[22] 是利用加密认证技术提出的另外一种改进方案。它通过在 ARP 消息中发布集中产生的〈IP，MAC〉地址映射证明（称之为票据），实现 ARP 报文的验证。这些票据由一个本地票据代理（local tickets agent，LTA）集中产生和标记，发送主机在 ARP 报文中附加上票据以便接收者进行验证。对于 TARP 协议的详细工作过程请参考文献[22]。TARP 协议与 ARP 协议兼容，但与安全 ARP 协议一样，也面临着 LTA 服务器单点故障和重放攻击的问题。

3.3　与 DHCP 协议相结合

Issac 等人[23] 提出一种与 DHCP 协议相结合的安全单播 ARP（S-UARP）协议，将基于广播的安全 ARP 协议（S-ARP）改进成一种单播协议。当局域网内的一台主机想与其他主机通信时，首先向支持安全单播 ARP 协议的 DHCP 服务器（称之为 DHCP＋）发送 S-UARP 请求报文，DHCP＋服务器查找它所分配的〈IP，MAC〉地址映射，发回相应的 S-UARP 应答报文；主机在收到应答报文后再向 DHCP＋服务器发送确认报文，安全单播 ARP 协议采用类似三次握手的方式完成 IP 地址和 MAC 地址的解析。为支持安全单播 ARP 协议，DHCP 代理也需要进行相应的修改。S-UARP 协议的优点是改进的单播协议避免了 ARP 欺骗的发生，减轻了局域网的 ARP 广播流量；缺点是为支持安全单播 ARP 协议，不仅需要改变 ARP 协议，还需要改进 DHCP 服务器和 DHCP 代理，实现比较复杂。而且 DHCP 服务器也面临着许多安全问题[24]，首先需要保证 DHCP 服务器的安全。

思科的动态 ARP 检查（dynamic ARP inspection，DAI）技术[25] 的提出利用 DHCP snooping 技术来监测与避免 ARP 欺骗，其工作流程如图 5 所示。交换机首先进行 DHCP snooping 监听，将主机从 DHCP 服务器获得的 IP 地址及其 MAC 地址保存到数据库（或文件）中，在接收到 ARP 请求报文时取出报文中的源 IP 地址与数据库中的记录进行比较，丢弃无效的 ARP 报文。DAI 技术无须修改 ARP 协议和 DHCP 服务器，但是需要部署支持 DHCP snooping 功能的交换机，经济成本比较高。目前其他厂家的交换机也具有利用 DHCP snooping 技术来避免发生 ARP 欺骗的功能[26]。

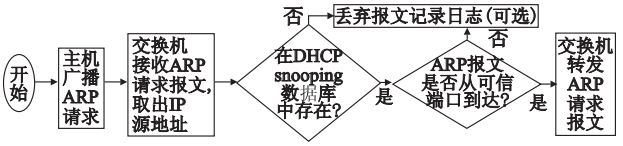

图5　动态ARP检查（DAI）的工作流程

4　现有技术的比较

表 2 对上面介绍的 ARP 欺骗监测和防范技术所采用的不同方法进行了简单总结。表 3 对其与 ARP 协议和 DHCP 协议的兼容性以及部署该技术对主机、交换机以及服务器的需求等方面进行了综合比较。通过分析和比较已有的 ARP 欺骗监测和防范技术可以发现，对于 ARP 欺骗，目前仍然没有完美的解决方案。

通过比较也可以看出，常规的 ARP 欺骗监测和防御技术由于方法简单，已经在局域网中得到应用，但是效果并不明显，不能从根本上避免 ARP 欺骗的发生。改进 ARP 协议的 ARP 欺骗避免技术则比较复杂，应用需求也比较多，其中基于中间件的方法需要修改系统内核，对于已经部署的数量庞大的主机和网络设备来说采用这种方法并不现实；采用安全认证技术的方法需要在局域网中增加集中式的安全服务器，这种方法具有一定的可行性，但是目前还没有得到实用；与 DHCP 服务相结合的方法则需要 DHCP 服务器和交换机的支持，由于这种方法得到了厂商的支持，在一些局域网中已经得到了部分应用[27]。ARP 欺骗避免技术对于主机、交换机和服务器的需求都很高，因此部署难度比较大，仍然需要进一步的研究和改进。

表 2　已有技术的简单总结

作用	技术	实现方法
监测	ARPWatch[9]	监听网络,监测可疑的〈IP,MAC〉地址映射改变,并通知网络管理员
	ARP-Guard[10]	采用分布式处理方法监听网络和利用 SNNP 探针监测可能发生的 ARP 欺骗
防御	ARP 防火墙[12]	安装在用户主机上,主动监测可能发生的 ARP 欺骗
	Port-Security[14]	限制交换机端口学习的 MAC 地址数量
	动态防御系统[15~17]	利用 SNMP 协议、脚本语言等方法动态监测存在的 ARP 欺骗,并采取相应的处理措施
避免	中间件技术[5]	修改内核,将无状态的 ARP 协议改进成有状态的协议
	Anticap[18]	修改内核,在请求 ARP 报文的〈IP,MAC〉地址映射与 ARP 缓存表不一致时拒绝刷新
	Gouda[19]	提出一种新的地址解析架构:安全服务器和新的地址解析协议
	S-ARP[20]	在局域网增加 AKD 服务器,采用非对称加密技术对 ARP 协议报文进行认证
	Goyal[21]	基于 S-ARP 协议,提高认证效率
	TARP[22]	利用 LTA 服务器集中产生的票据,对 ARP 报文进行验证
	S-UARP[23]	提出安全单播 ARP 协议,需要 DHCP + 服务器和 DHCP 代理支持该协议
	DAI[25]	需要交换机支持,利用 DHCP snooping 记录 DHCP 服务器分配的〈IP,MAC〉地址映射,与请求 ARP 报文的 IP 源地址相比较

表 3　兼容性与应用需求的比较

技术	ARP 兼容性	DHCP 兼容性	主机需求	交换机需求	服务器需求
ARPWatch	√	√		端口镜像	数据库服务器
ARP-Guard	√	√		端口镜像,支持 SNMP	数据库服务器
ARP 防火墙	√	√	安装软件		
Port-Security	√	√		支持 Port-Security	
动态防御系统	√	√		端口镜像,支持 SNMP	数据库服务器
中间件技术	√	√	修改内核		
Anticap	√		修改内核		
Gouda			修改内核	支持新协议	安全服务器
S-ARP	√	√	修改内核		AKD 服务器
Goyal	√	√	修改内核		AKD 服务器
TARP	√	√	修改内核		LTA 服务器
S-UARP		√	修改内核	支持新协议	DHCP + 服务器
DAI	√	√		支持 DHCP-snooping	DHCP 服务器

下一步研究和改进 ARP 协议,需要综合考虑下面一些因素,在避免发生 ARP 欺骗的条件下取得理想的应用效果:

a)兼容性。ARP 协议作为 TCP/IP 协议族的一员,已经得到了广泛的部署。对 ARP 协议的改变意味着需要对成千上万台主机和网络设备进行修改。因此改进 ARP 协议首先要保证兼容 ARP 协议,无须修改现有主机和网络设备。

b)透明性。改进的 ARP 协议对用户透明,无须用户参与,保留用户原有的操作习惯。

c)系统和网络开销。改进的 ARP 协议对主机性能没有影响或影响很小,且消息交互过程不会产生很大的网络流量。更重要的是,部署改进的 ARP 协议对主机、网络设备和服务器的需求要少,以尽可能地减少系统和网络开销。

5　结束语

本文简要介绍了 ARP 协议的工作流程,阐述了 ARP 欺骗产生的原理以及攻击形式,并对已有的针对 ARP 欺骗的监测、防御与避免技术进行分类和总结;着重介绍了其工作原理和优缺点,并提出研究改进 ARP 协议需要综合考虑的因素。下一步工作将重点研究改进 ARP 协议,探讨可信任的安全局域网的设计与实现。

参考文献:

[1] BUER S. Arpoison[EB/OL]. [2008-04-10]. http://arpoison.sourceforge.net.

[2] SONG D. Dsniff: a collection of tools for network auditing and penetration testing[EB/OL]. (2005-06)[2008-04-10]. http://naughty.monkey.org/~dugsong/dsniff/.

[3] 郑先伟. Cernet 应急响应组 2007 年 5 月报告:ARP 欺骗是首要威胁[J]. 中国教育网络,2007(7):41-43.

[4] PLUMMER D C. RFC 826, An Ethernet address resolution protocol[S]. 1982.

[5] TRIPUNITARA M V, DUTTA P. A middleware approach to asynchronous and backward compatible detection and prevention of ARP cache poisoning[C]//Proc of the 15th Annual Computer Security Applications Conference. Washington DC: IEEE Computer Society, 1999:303-309.

[6] WHALEN S. An introduction to ARP spoofing[EB/OL]. (2001-04). http://www.rootsecure.net/content/dcunloads/pdf/arp_spoofing_intro.pdf.

[7] 赵春华. ARP 欺骗分析、处理及防范[J]. 金融电子化,2007(12):53-54.

[8] Ethereal: a network protocol analyzer[EB/OL]. (2006-05)[2008-04-10]. http://www.ethereal.com.

[9] GROUP L N R. Arpwatch, the Ethernet monitor program for keeping track of Ethernet/IP address pairings[EB/OL]. (2005-05)[2008-04-10]. ftp://ftp.ee.lbl.gov/arpwatch.tar.gz.

[10] ARP-Guard[EB/OL]. (2008-01)[2008-04-10]. http://www.arp-guard.com.

[11] Snort Project. The Snort: the open source network intrusion detection system[EB/OL]. [2008-04-10]. http://www.snort.org.

[12] ARP 防火墙[EB/OL]. (2008-01-30)[2008-04-10]. http://www.antiarp.com.

[13] 庆秋辉,徐同阁. MAC-IP 地址绑定的一种软件实现方法[J]. 现代电子技术,2006,29(8):74-77.

[14] SCHLUTING C. Configure your catalyst for a more secure layer 2 network[EB/OL]. (2005-01)[2008-04-10]. http://www.enterprisenetworkingplanet.com/netsecur/article.php/3462211.

[15] 吴小平,周建中,方晓惠. 基于 SNMP 的 ARP 欺骗主动防御机制[J]. 华中师范大学学报:自然科学版,2007,41(4):512-514.

[16] 陈文波,李善玺. 针对 ARP 欺骗的动态检测防御系统[J]. 中国教育网络,2007(8):76-77.

[17] 陈辉,陶洋. 基于 WinPcap 实现对 ARP 欺骗的检测和恢复[J]. 计算机应用,2004,24(10):65-67,85.

[18] BARNABA M. Anticap[EB/OL]. (2003-03)[2008-04-10]. http://www.antifork.org/viewcvs/trunk/anticap.

[19] GOUDA M G, HUANG C T. A secure address resolution protocol[J]. Computer Networks,2003,41(1):57-71.

[20] BRUSCHI D, ORNAGHI A, ROSTI E. S-ARP: a secure address resolution protocol[C]//Proc of the 19th Computer Security Applications Conference. Washington DC: IEEE Computer Society, 2003:66-74.

[21] GOYAL V, ABRAHAM A. An efficient solution to the ARP cache poisoning problem[C]//Proc of the 10th Australasian Conference on Information Security and Privacy. Berlin: Springer, 2005:40-51.

[22] LOOTAH W, ENCK W, McDANIEL P. TARP: ticket-based address resolution protocol[C]//Proc of the 21st Annual Computer Security Applications Conference. 2005:106-116.

[23] ISSAC B, MOHAMMED L A. Secure unicast address resolution protocol (S-UARP) by extending DHCP[C]//Proc of the 13th IEEE International Conference on Networks. 2005.

[24] DHCP: another untrustworthy service[EB/OL]. [2008-04-10]. http://www.spirit.com/Network/net0202.html.

[25] Cisco System. Catalyst 6500 series switch Cisco IOS software configuration guide, Release 12.2SX[K]. 2006.

[26] 杨名川. 利用华为交换机防止 ARP 欺骗[J]. 现代计算机,2007(2):110-112.

[27] 陈伟斌,薛芳,任勤生. ARP 欺骗攻击的整网解决方案研究[J]. 厦门大学学报:自然科学版,2007,46(S-2):100-103.

[28] 徐丹黎,俊伟,高传善. 基于 Ethernet 的网络监听以及 ARP 欺骗[J]. 计算机应用与软件,2005,22(11):105-107.