利用 ARP 伪装在交换以太网捕包

贺龙涛　方滨兴　云晓春　汪立东
哈尔滨工业大学计算机科学与技术学院　黑龙江·哈尔滨　150001

摘　要　本文分析了以太网捕包技术，并对在交换型以太网络进行捕包的可能性进行探讨，在详细研究了 ARP 协议之后，提出了利用 ARP 伪装攻击结合 IP 转发技术来进行捕包的主动捕包技术。

关键词　交换网络，ARP 伪装，IP 转发，主动捕包

1. 引言

网络捕包，即将网络上传输的数据捕获的行为。在网络安全领域，网络捕包占有极其重要的作用。对于黑客攻击而言，网络捕包是一种有效的信息（用户名、口令等）收集手段，并且可以辅助进行 IP 欺骗[1]；对于安全管理而言，捕包也是监控本地网络状况的直接手段，捕包还是基于网络的入侵检测系统（NIDS）的必要基础[2] 。然而，通常意义上的网络捕包，是有一定先决条件的：那就是捕包必须是在广播式网络环境下进行，而对于交换式以太网络环境，即使是将网卡设置成混杂模式，依旧只能捕获本该到达该以太地址的数据包。

本文对在交换以太网下进行捕包的可能性进行研究，并提出了一个可用的捕包方法。

2. ARP 协议分析

2.1 ARP 协议简介

在 TCP/IP 协议中，数据链路层如以太网或令牌环网都有自己的寻址机制（常常为 48bit 地址），这是使用数据链路的任何网络层都必须遵从的。一个网络如以太网可以同时被不同的网络层使用。当一台主机把以太网数据帧发送到位于同一局域网上的另一台主机时，是根据 48bit 的以太网地址来确定目的接口的。设备驱动程序从不检查 IP 数据报中的目的 IP 地址。这就存在一个如何将 32bit 的 IP 地址和数据链路层使用的地址进行映射的问题。

ARP（地址解析协议）[3]正是完成这样工作的协议。ARP 为 IP 地址到对应的硬件地址之间提供动态映射，这个过程是自动完成的，一般应用程序、用户或系统管理员不必关心。

在 ARP 背后有一个基本概念，那就是网络接口有一个硬件地址（一个 48bit 的值，标识不同的以太网或令牌环网络接口）。在硬件层次上进行的数据帧交换必须有正确的接口地址。但是，TCP/IP 有自己的地址：32bit 的 IP 地址。知道主机的 IP 地址并不能让内核发送一帧数据给主机。内核（如以太网驱动程序）必须知道目的端的硬件地址才能发送数据。ARP 的功能是在 32bit 的 IP 地址和采用不同网络技术的硬件地址之间提供动态映射。

2.2 ARP 的工作过程

如图 1 所示，在应用程序请求 TCP 用域名解析得到的 IP 地址建立连接时，会进行以下这些步骤[4]：

1）　TCP 发送一个连接请求分段到远端的主机，即用上述 IP 地址发送一份 IP 数据报。

2）　如果目的主机在本地网络上（如以太网、令牌环网或点对点链接的另一端），那么 IP 数据报可以直接送到目的主机上。如果目的主机在一个远程网络上，那么就通过 IP 选路函数来确定位于本地网络上的下一站路由器地址，并让它转发 IP 数据报。在这两种情况下，IP 数据报都是被送到位于本地

*国防科技预研跨行业综合技术项目计算机病毒及其预防技术(编号 15.7.2)

作者简介：贺龙涛，男，1974 年生，博士研究生，研究方向：计算机网络与信息安全，网络应用技术，方滨兴，博士生导师，研究方向：计算机网络与信息安全，并行计算，体系结构。

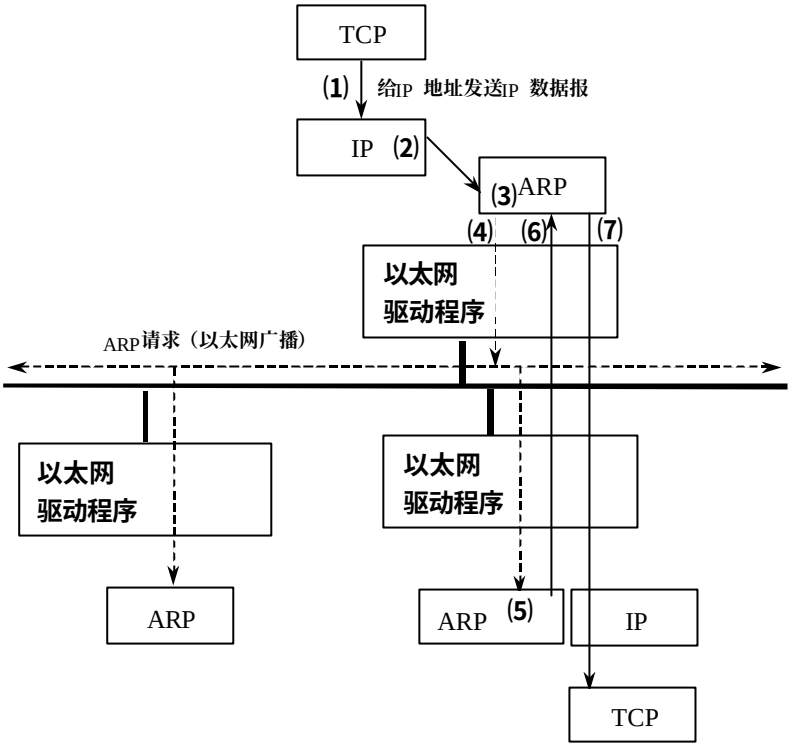

图 1 ARP 的工作过程

网络上的一台主机或路由器。

3） 假定是一个以太网，那么发送端主机必须把 32bit 的 IP 地址变换成 48bit 的以太网地址。ARP 的功能就是从逻辑 Internet 地址到对应的物理硬件地址需要进行翻译。

4） ARP 发送一份称作 ARP 请求的以太网数据帧给以太网上的每个主机。这个过程称作广播，如图 1 中的虚线所示。ARP 请求数据帧中包含目的主机的 IP 地址，其意思是“ 如果你是这个 IP 地址的拥有者，请回答你的硬件地址。”

5） 目的主机的 ARP 层收到这份广播报文后，识别出这是发送端在寻问它的 IP 地址，于是发送一个 ARP 应答。这个 ARP 应答包含 IP 地址及对应的硬件地址。

6） 收到 ARP 应答后，该 IP 数据报所需的目的硬件地址就知道了，就可以传送该报文了。

7） 发送 IP 数据报到目的主机。

2.3 ARP 的分组格式

在以太网上解析 IP 地址时，ARP 请求和应答分组的格式如图 2 所示（ARP 可以用于其他类型的网络，可以解析 IP 地址以外的

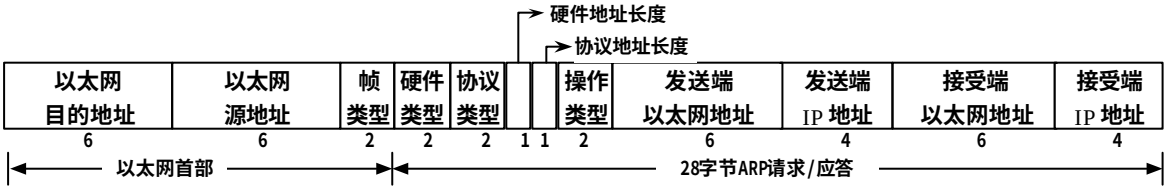

图2 用于以太网的ARP请求或应答分组格式

地址。紧跟着帧类型字段的前四个字段指定了最后四个字段的类型和长度）。

以太网报头中的前两个字段是以太网的目的地址和源地址。目的地址为全 1 的特殊地址是广播地址。同一局域网上的所有以太网接口都要接收广播数据帧。接着是以太网帧类型，2 字节长，表示后面数据的类型。对于 ARP 请求或应答来说，该字段的值为 0x0806。

硬件类型字段表示硬件地址的类型。值为 1 即表示以太网地址。协议类型字段表示要映射的协议地址类型。值为 0x0800 即表示 IP 地址。

硬件地址长度和协议地址长度分别指出硬件地址和协议地址的长度，以字节为单位。对于以太网上 IP 地址的 ARP 请求或应答来说，它们的值分别为 6 和 4 。

操作字段指出操作类型，可以为 ARP 请求（值为 1）、ARP 应答（值为 2）。

其余的四个字段是发送端的硬件地址（以太网地址）、发送端的协议地址（IP 地址）、目的端的硬件地址和目的端的协议地址。

对于 ARP 请求来说，除目的端硬件地址外的所有其他的字段都有填充值。当系统收到一份目的端为本机的 ARP 请求报文后，它就把硬件地址填进去，然后用两个目的端地址分别替换两个发送端地址，并把操作字段置为 2，最后把它发送回去。

2.3 ARP 高速缓存

ARP 高效运行的关键是由于每个主机上都有一个 ARP 高速缓存。这个高速缓存存放了最近 IP 地址到硬件地址之间的映射记录。高速缓存中每一项的生存时间一般为 20 分钟。

3. 利用 ARP 伪装在交换以太网下进行捕包

3.1 ARP 协议弱点分析

由以上可知，ARP 协议虽然是一个高效的数据链路层协议，但是作为一个局域网协议，它是建立在各主机之间相互信任的基础上的，因此有不少安全问题：

1． 主机地址映射表是基于高速缓存，动态更新的。这是 ARP 协议的特色之一，但也是安全问题之一，由于正常的主机间的 MAC 地址刷新都是有时限的，这样假冒者如果在下次交换之前成功地修改了被攻击机器上的地址缓存，就可以进行假冒或者拒绝服务攻击了。

2． ARP 请求是以广播方式进行的。这个问题是不可避免的，因为正是由于主机不知道通信对端的 MAC 地址，才需要进行 ARP 广播请求的。这样，攻击者就可以伪装 ARP 应答，与广播者真正要通信的机器进行竞争。还可以确定子网内机器什么时候会刷新 MAC 地址缓存，以确保最大时间限度地进行假冒。

3． 可以随意发送 ARP 应答包。这是由于 ARP 协议是无状态的，任何主机即使在没有请求的时候也可以做出应答，所以任何时候都可以发送 ARP 应答，只要应答包是有效的，接收到 ARP 应答的主机就无条件的根据应答包的内容刷新本机高速缓存。

4． ARP 应答无需认证。由于 ARP 协议是一个局域网协议，一般来讲，一个局域网内的主机都是属于同一个组织的，主机间的通信基本上是相互信任，独立自治的，在出于传输效率上的考虑，在数据链路层就没做什么安全上的考虑，在使用 ARP 协议交换 MAC 地址时，无需认证，只要是收到来自局域网内的 ARP 应答包，就将其中的 MAC /IP 地址对刷新到本主机的高速缓存中。

3.2 ARP 欺骗攻击

根据以上的讨论，可以使用以下几种手段来进行 ARP 欺骗：

1．如图 1，在以上 2.2 节介绍的 ARP 工作过程中，第 4 步是进行 ARP 广播请求，这样攻击者也就可以在接收到该 ARP 请求包之后进行应答，进行假冒。

2．由于被假冒的机器所发送的 ARP 应答包有可能比攻击者的应答包晚到达，为了确保被攻击者机器上的缓存中绝大部分时间存放的是攻击者的 MAC 地址，可以在收到 ARP 请求广播后稍微延迟一段时间再发送一遍 ARP 应答。

3．由于各种操作系统对于 ARP 缓存处理实现的不同，一些操作系统（例如 Linux）会用向缓存地址发非广播的 ARP 请求来要求更新缓存。在交换网络环境下，别的机器是不能捕获到这种缓存更新的，这就需要尽量阻止主机发送更新缓存消息，由 3.1 小节的第 3 条分析知道，可以随意发送 ARP 应答包，这样攻击者就可以定时发送 ARP 应答包，不断的更新被攻击者的 MAC 缓存，阻止它主动发送非广播的 ARP 请求进行缓存更新。

3.3 IP 包转发

以上已经可以使子网内的别的机器的网络流量都会流到攻击者机器来，为了使他们还能够“正常”地使用网络，攻击者就必须将他们的数据包转发到他们真正应该到达的主机去，这就需要进行转发，本文主要考虑 IP 包的转发。

IP 包转发，实质上是和路由器的工作基本相同的，区别只是在于路由器是在不同局域网之间进行包转发，而这里的 IP 包转发

只是在局域网内进行转发。

已经由许多工具可以进行 IP 转发，本文对只是作一个简单的实现：

1． 保持一个局域网内各个 IP/MAC 的对应列表，根据捕获的 IP 包或者 ARP 包的源 IP 域进行更新。

2． 收到一个 IP 分片包之后，分析 IP 包头，根据 IP 包头里目的 IP，找到相应的 MAC 地址。

3． 将本机的 MAC 地址设成源 MAC，第二步查找到的 MAC 地址作为目的 MAC，将收到的 IP 分片包写到网卡。

3.4 ARP 欺骗与 IP 转发的结合

由以上的介绍可知，要使用 ARP 欺骗结合 IP 转发的发式来进行捕包，可以使用两个线程：一个进行捕包分析，一个定时发送 ARP 应答包，它们依靠一个全局的 IP/MAC 地址对应列表来交互。

捕包进程的主要流程：

```
while(true)
{
    接收到一个以太包；
    进行捕包相关处理；
    if（是本机发出的包 || 到达本 IP 的包）
        return;
    if（是 ARP 请求包）
    {
        发送伪造的 ARP 应答包；
        在 IP/MAC 表中作相应修改；
        return;
    }
    if（是 IP 分片包）
    {
        在 IP/MAC 中查找目的 IP 的 MAC 地址；
        重新填写所捕获包的以太头部分并发送；
        return;
    }
}
```

定时进程的主要流程：

```
while(true)
{
    睡眠一定时间；
    按照 IP/MAC 列表轮发送伪造的 ARP 应答包；
}
```

4. 结束语

网络捕包对黑客技术与安全管理都是十分重要的，本文提出了主动捕包的思想，打破了交换网络不能进行捕包的传统概念，并实现了一个使用 ARP 欺骗与 IP 转发相结合的主动捕包系统。

参考文献

1. Brecht Claerhout. A short overview of IP spoofing. Phrack Magazine. 1996, 7(48)
2. Mark Crosbie, Gene Spafford. Defending A Computer System using Autonomous Agents. COAST Laboratory. March 11, 1994
3. David C. Plummer. RFC826
4. Gary R. Wright, W. Richard Stevens. TCP/IP Illustrated volume 1: The Protocol. Addison Wesley Publishing Company. 1994
5. S.M. Bellovin. Security Problems in TCP/IP Protocol Suite. Computer Communication Review, Vol. 19, No.2, April 1989

Sniffing in Switched Ethernet with ARP Spoofing

He Longtao Fang Binxing Yun Xiaochun Wang Lidong

(Dept. of Computer Science and Engineering, Harbin Institute of Technology, Harbin 150001)

Abstract

The sniffing in ether network is analyzed, then the possibility of sniffing in switched ether network is studied. After ARP protocol is stutied in details, an active

sniffing technique is put forward, which combines ARP spoofing and IP forwarding.
Key words: Switched Network, ARP Spoofing, IP Forwarding, Active Sniffing