摘要：本文在分析了ARP协议的工作原理后，对ARP协议在以太网中的存在的漏洞进行了较详细的分析，最后提出了一些防范的建议和思路。

关键词：ARP　ARP欺骗　IP转发

ARP协议的安全漏洞及其防范浅析

Brief Analysis of Security Flaw of ARP Protocol and the Countermeasures

罗杰云 （广东省江门市五邑大学　529020） 倪德明 （中山大学软件研究所　510275）

1 引言

随着计算机在人类生活各领域中的广泛应用，计算机网络对社会活动的影响已经渗透到各个方面，网络信息的安全也成为一个越来越引起世界各国关注的复杂问题。网络功击、黑客充斥着网络世界。人们有必要从根本上、理论上认识网络安全漏洞所在。本文从一个侧面分析了ARP协议的安全漏洞，提出了相应的防范建议。

2 ARP协议的分析

网络攻击的一种最主要的形式是对网络协议弱点的攻击。当初设计Internet各类协议时，几乎没有人考虑网络安全问题，网络协议或缺乏认证机制，或缺少数据保密性。因此，Internet作为TCP/IP的第五层结构，从数据链路层到应用层协议在设计上都存在不同程度的安全漏洞，可能被攻击者加以利用而入侵网络。

2.1 ARP协议的含义、作用

ARP协议是TCP/IP协议栈的基础协议之一，ARP提供地址解析服务，用于将32位IP地址映射到以太网的48位硬件地址（也称MAC地址），以便将IP报文封装成以太帧发送。

ARP协议功能主要是将上层的IP地址与下层的物理地址进行绑定，ARP协议形成了只能使用IP地址的上层协议软件与只能使用物理地址的下层设备驱动程序软件之间的分界线，这样ARP协议就使高层协议与物理地址无关。

2.2 ARP协议的工作原理

以太网：源主机与目的主机在同一个子网

(1) 第一种情况：源主机与目的主机在同一个子网内。(如图1)

① 当源主机A(IP地址为：197.15.22.11,子网掩码：255.255.255.0)需要和目标主机D (IP地址为：197.15.22.44，子网掩码：255.255.255.0) 通信时，主机A必须知道主机D的MAC地址。如果它在自己的ARP表中找不到目标主机D的MAC地址，主机A发出一个ARP请求的以太网数据帧广播给子网内的每一个主机。

以太网帧的MAC地址头部为：

目标地址：FF-FF-FF-FF-FF-FF

源 地 址：02-60-8C-01-02-03

以太网帧的IP地址头部为：

目标地址：197.15.22.44

源地址：197.15.22.11

帧的内容含义为：如果你的IP地址是：197.15.22.44，请回答你的MAC地址。

② 当目的主机D收到这份报文后，能识别出这是寻问IP地址到MAC地址的映射，之后发送一个ARP应答。这个应答包含IP地址及对应的MAC地址。

③ 源主机收到应答后，即可从中抽取所需的目的主机的MAC地址。

(2) 第二种情况：源主机与目的主机不在同一个子网内。(如图2)

我们知道，当一主机和不在同一子网内的另一个主机通信时，必须提供一个缺省网关。即：路由器中与该主机连在同一子网的端口IP地址。

① 当源主机A(IP地址为：197.15.22.11,子网掩码：255.255.255.0)需要

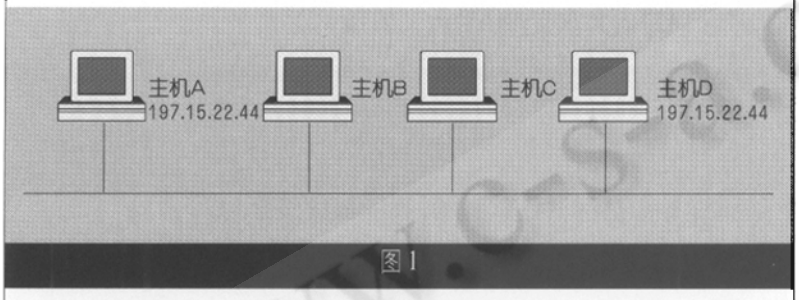

图1

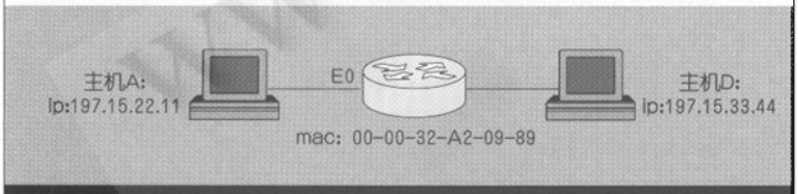

图2

和目标主机D (IP地址为：197.15.33.44,子网掩码：255.255.255.0) 通信时，用目标主机IP地址与自己的子网掩码进行与运算，发现目标主机IP属于子网197.15.33.0，而自己属于子网197.15.22.0。

② 此时，源主机就用路由器端口E1的MAC地址00-00-32-A2---09-89作为目标MAC地址。

2.3 ARP报文格式

ARP请求和应答报文的格式如图3所示。

硬件类型字段指明了发送方想知道的硬件接口类型：以太网的值为1.协议类型字段指明了要映射的协议地址类型.值为0X0800即为IP地址。硬件地址长度和协议地址长度字段允许ARP在任意网络中使用。对于以太网上IP地址的ARP或应答来说，它们的值为6和4.操作类型指明一个操作类型--ARP请求（值为1）、ARP应答（值为2）、RARP请求（值为3）、RARP应答（值为4）。其余的四个字段是发送方的硬件地址与发送方的协议地址（IP地址）、接收方的硬件地址与发送方的协议地址（IP地址）。

当发送方发出ARP请求时，其报文内容中留出目标主机的硬件地址字段。在目标主机响应之前，它填好所缺的硬件地址，交换接收方和发送地址对的位置，并把操作改成应答。

3 ARP高速缓存的管理

(1) ARP高速运行的关键是由于每个主机都有一个ARP高速缓存。最近的IP地址与MAC地址映射表就存放在这高速缓存中。高速缓存中的IP/MAC映射表的每一个表项均有一个生存期。

(2) ARP高速缓存管理程序每隔一固定时间检查高速缓存中所有的表项，并删除已达到时限的表项。

(3) 协议规定，如果到达的是一个ARP请求分组，即使接收方并没有等待此地址转换的表项，接收方也必须在其高速缓存中增加或更新这个发送方的IP到MAC地址的映射信息。

(4) 协议还规定，如果到达的是一个ARP应答分组，接收方就直接在其高速缓存中更新其中的IP到MAC地址的映射信息。

(5) 如果一个IP进程需要发送一份数据报，但其目的地址不在ARP高速缓存的任何一个表项中，则IP必须创建一个新表项。在为高速缓存中的新成员分配空间时，如果存在一个空闲表项，就选择此空闲表项。否则，采用一替换策略删除旧表项。

4 ARP协议漏洞分析

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，因此存在一些安全问题：

(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MAC地址刷新都是

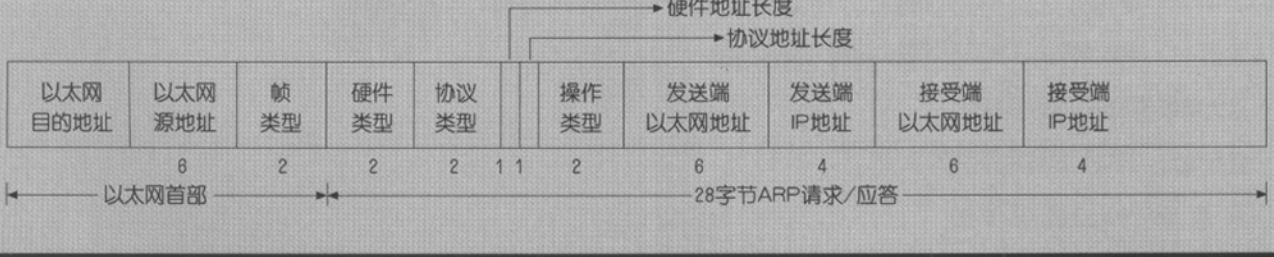

图3

有时限的，这样假冒者如果在下次更新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请求以广播方式进行。这个问题是不可避免的，因为正是由于主机不知道通信对方的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，只要应答包是有效的，接收到ARP应答包的主机就无条件地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协议是一局域网协议，一般来讲，一个局域网内的主机是属于同一个组织的，主机间的通信是相互信任，，出于传输效率上的考虑，在数据链路层就没做安全上的考虑。在使用ARP协议交换MAC协议时，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协议对刷新到本主机的高速缓存中。

5 ARP欺骗攻击

根据以上的分析，攻击者利用ARP的弱点可以进行阻止或破坏双方通信、拒绝服务、网络信息的截获以及IP包的转发等攻击活动。常采用以下几种手段来进行ARP欺骗：

(1) 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协议，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。

(2) 由于各种操作系统对于ARP缓存处理实现的不同，一些操作系统会向缓存地址发送非广播的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更新缓存信息。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) 在ARP表中的每一个条目都有一个计时器，如果计时器过期，该条目就无效，而从缓存中被删除。如果攻击者暂时使用不工作的主机的IP地址，就可以伪造IP/MAC地址对，把自己伪装成那个暂时不使用的主机一样。

(4) 攻击者可以阻止或破坏双方通信。由于高速缓存是动态更新的，攻击者定时地发送ARP应答包，其发送时间间隔较短，远小于动态更新的时间（即表项的生存期）。这样，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。

6 ARP欺骗的隐蔽性分析

(1) 通过以上的有关对ARP欺骗分析，可以使子网内的其他机器的网络流量都回流到攻击者机器来，为了隐蔽自己，它必须使他们（被攻击者）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，这需要进行IP包的转发。ARP欺骗的隐蔽性是通过IP包的转发来实现。

(2) 包的转发的实现：

① 保持一个局域网内各个IP/MAC包的对应列表，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包头里的目的IP，找到相应的MAC地址。

③ 将本机的MAC地址设成源MAC地址，将第二步查找到的MAC地址作为目的MAC地址，将收到的IP分片包发送出去

7 常见防范措施

主要是采用硬件方法，将网络分段来达到防止ARP欺骗功击目的。利用多层交换机、动态集线器和桥等设备对数据流进行限制。

由于在共享介质环境下，如果使用的是一般的集线器或集中器，要插入一个新接点非常容易，这样数据包很容易被探测，实现ARP欺骗功击。利用交换机等设备具有管理端口及节点的MAC地址功能的特点，将网络进行分段，如图4。该交换机知道所连主机的MAC地址，并将这些MAC地址及其对应的端口保存在内部表格中。当某个端口接收到包时，交换机会将包中记录的源地址与端口读到的源地址进行比较。如果源地址发生了改变，一个通知被发送到管理工作站，该端口被自动禁止直到冲突解决为止。

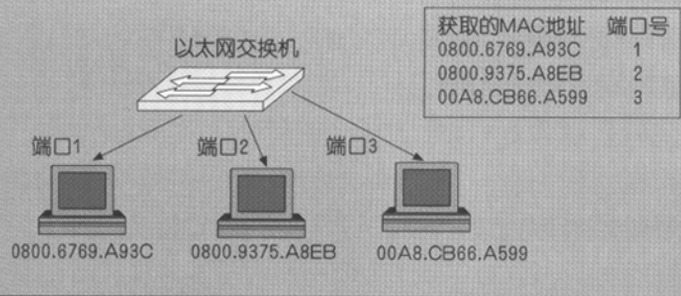

图4

参考文献

1 谢希仁，计算机网络 [M]，电子工业出版社，1999。

2 Douglas E.comer 用TCP/IP进行网际互联，第一卷，电子工业出版社，2001。

3 David C.plummer. RFC826。

4 S.M.Bellovin. Security Problems in TCP/IP Protocol Suite.Bell laboratories。