ARP 协议的安全漏洞及抵御分析①

李 兢 许 勇 (桂林电子科技大学 计算机与控制学院 广西 桂林 541004)

摘 要: 介绍了 ARP 协议的功能和工作原理基础上，分析了当前 ARP 协议所存在的安全漏洞。重点讨论了利用 ARP 协议自身的安全缺陷进行网络攻击的多种实现方法以及这些攻击所带来的危害。最后根据实际的管理，给出了一些有效的安全抵御措施和检测方法，并说明了这些方法的优点与缺点。

关键词: ARP 协议；安全缺陷；防范措施；检测方法

A Brief Analysis of Security Flaws in ARP Protocol and Protecting Project

LI Jing, XU Yong

(Computer and Control College, Guilin University of Electronic Technology, Guilin 541004, China)

Abstract: Based on an introduction to the functions and working theory of the ARP (Address Resolution Protocol), this paper analyses the security holes in ARP. The security vulnerability of ARP, the attacking forms and potential damages are extensively discussed. Several protection solutions for daily managements and detection are given, advantages and disadvantage of these measures are detailed.

Keyword: ARP; security vulnerabilities; protection measures; detection method

1 ARP协议介绍

ARP 协议(Address Resolution Protocol)也就是地址解析协议，是由 David C.Plummer 在 826 internet 标准（草案）提出，当时是为了美国数字设备公司、英特尔公司、施乐复印机公司等三个公司的 10 Mbit 以太网所设计，在推广时也允许其它类型的网络使用。ARP 协议工作在 TCP/IP 的 IP 层。在 IPv4 中，ARP 是一种将网络层 IP 地址转化成物理 MAC 地址的协议，这种映射的过程非常重要，它是传输 IP 数据包不可缺少的过程。

2 ARP工作原理

在网络中的任何一台主机，都有两个唯一的标识。一个是由 32 位二进制组成的 IP 地址，用于在网络层当中标识和查找计算机，另一个是由 48 位二进制组成的 MAC 地址，用于在数据链路层中标识和查找计算机。IP 地址是不能直接用来通讯的，因为 IP 地址只是主机在网络层中的地址，如果要将网络层中传输的数据报交给目的主机，还要传到链路层变成 MAC 帧才能发送到实际的网络上。因此 IP 地址与 MAC 地址之间就必须存在一个映射表，而 ARP 协议就很好的解决了这些问题。

每一台安装有 TCP/IP 协议的计算机内部都有一张 ARP 高速缓存表，该缓存表记录了最近一段时间内区域网内与该计算机通讯的其他计算机的 IP 地址与其相应的 MAC 地址之间的对应关系。

当源主机要发送 IP 数据报时，数据链路层必须将 IP 数据报封装成以太网数据帧，才能在以太网中传输。在封装过程中，为了找到与目的 IP 地址对应的 MAC 地址，源主机先会把目的主机的 IP 的地址与子网掩码进行逻辑与操作，以判断目的主机是否与自己在同一个网段内。如果在同一网段内，源主机会先查看 ARP 高速缓存是否有与目的IP地址对应的MAC地址信息，如果 MAC 地址已存在，就直接使用。如果对应的信息不存在，就向本地网段发起一个包含 ARP 请求的广播包，查询此目的主机对应的 MAC 地址。此 ARP 请

① 收稿时间:2009-07-20

求数据包里包括源主机的 IP 地址、MAC 地址、以及目的主机的 IP 地址。网络中所有的主机收到这个 ARP 请求后，会检查数据包中的目的 IP 是否和自己的 IP 地址一致。如果不相同就忽略此数据包，如果相同，则给源主机发送一个 ARP 响应数据包，通过该报文使源主机获得目标主机的 MAC 地址信息则可利用此信息开始数据的传输。假如目的主机与源主机不在同一个网段内，源主机会在 ARP 高速缓存中查找默认网关所对应的 MAC 地址，由默认网关再对该分组进行转发。如果没有，源主机就会发送一个广播包，查询默认网关对应的 MAC 地址。主机每隔一段时间或者每收到新的 ARP 应答就会更新 ARP 缓存，以保证自己拥有最新的地址解析缓存。

3 ARP协议的漏洞

ARP 协议是建立在信任局域网内所有结点的基础上的，它很高效，但却不安全。它的主要漏洞有以下三点。

(1) 主机地址映射表是基于高速缓存、动态更新的，ARP 将保存在高速缓存中的每一个映射地址项目都设置了生存时间，它只保存最近的地址对应关系。这样恶意的用户如果在下次交换前修改了被欺骗机器上的地址缓存，就可以进行假冒或拒绝服务攻击。

(2) 由于 ARP 是无状态的协议，即使没有发送 ARP 请求报文，主机也可以接收 ARP 应答，只要接受到 ARP 应答分组的主机就无条件地根据应答分组的内容刷新本机的高速缓存。这就为 ARP 欺骗提供了可能，恶意节点可以发布虚假的 ARP 报文从而影响网内结点的通信，甚至可以做“中间人”。

(3) 任何 ARP 应答都是合法的，ARP 应答无须认证，只要是区域网内的 ARP 应答分组，不管(其实也不知道)是否是合法的应答，主机都会接受 ARP 应答，并用其 IP－MAC 信息篡改其缓存。这是 ARP 的另一个隐患。

4 ARP进攻分类

4.1 ARP spoof 攻击

“中间人”攻击，又称为 ARP 双向欺骗。它的基本原理就是将自己的主机插入到两个目标主机通讯路径之间，截获两个目的主机直接的通讯数据。假设有三台主机(如图 1 所示)，正常下 A 与 C 直接的通讯是不可见的，但是利用“中间人”的欺骗技术，主机 B 可以实现交换机网络下的嗅探。其主要步骤如下：

(1) 主机B向主机A发送一个非法的ARP响应包，里面包括主机 C 的 IP 地址和主机 B 的 MAC 地址，主机 A 收到这个包后并没有去验证包的真实性就把 ARP 缓存中 C 的地址篡改为 B 的 MAC 地址。

(2) 主机 B 也向主机 C 发送一个非法的 ARP 包，里面包含了 A 的 IP 地址和 B 的 MAC 地址，由于 ARP 协议的漏洞，主机 C 也没有验证 ARP 的真实性就把 ARP 缓存中 A 的 MAC 地址改为 B 的 MAC 地址。

(3) 主机 B 启动 IP 转发功能。

主机 A 与 C 的所有直接的通讯将经过 B，再由 B 转发给他们。这样主机 B 就成功的对网内的用户进行了 ARP 欺骗。

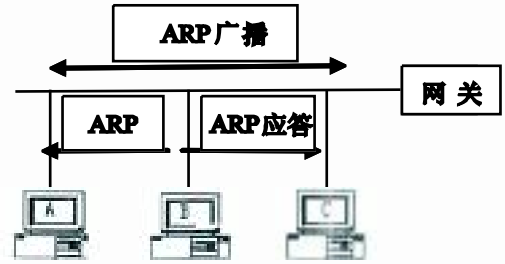

图 1　ARP 欺骗的过程

4.2 网络监听

由图 1 可知，当攻击者 B 想要截取主机 C 对外网通讯的信息时，主机 B 会给主机 C 和网关 D 发送一个欺骗的 ARP 应答包，根据“中间人”的欺骗原理，主机 C 和网关 D 都会认为主机 B 是对方，这样主机 C 看似能于外网进行通讯了，然而实际上它的通讯信息却受到主机 B 的监听。此时，主机 B 不仅可以完成监听，还可以随意改变数据包中的信息，并成功转发数据包。假如主机 B 在区域网上广播一个 IP 地址为网关的欺骗 ARP 通知包，并篡改网关 D 的 ARP 缓存内的 IP-MAC 映射，主机 B 则可以监听区域网内与外网的所有通讯信息。大部分的木马或病毒都使用该 ARP 欺骗攻击手段到达攻击的目的。

4.3 广泛拒绝服务攻击 DOS

拒绝服务攻击 DOS 就是使目标主机不能正常响应外界请求，不能对外提供服务。拒绝服务攻击主要有以下 4 种方式：

(1) 进攻主机持续响应本网络内的所有 ARP 应答，并且应答为一个虚构的 MAC 地址，那么目的主机向外发送的所有数据帧都会丢失，使得上层应用忙于处理这种异常而无法响应外来请求,也就导致目标主机产生拒绝服务。

(2) 进攻主机持续响应本网络所有的 ARP 进行应答，并且应答包内的 MAC 地址全部为本子网网关的 MAC 地址，由于网关自身有 IP 转发功能的，那么本子网内所有的数据通讯都需要网关进行一次转发，这样就无形中增加了网关的负荷，会导致网关超负荷而崩溃或者等待队列过长，进而使子网主机内部之间，子网主机与外网主机之间的通讯全部失败或者收发数据超时。

(3) 一般交换网络采用的多是二层交换机，此类交换机自身维护着一个 ARP 缓存，用于映射 MAC 地址对应的交换机的端口号，这个缓存中可容纳的映射条数是有限的[1]。如果进攻主机发送大量的包含不同 MAC 地址的 ARP 包，当数量足够多时，就有可能造成交换机 DOS，不能正常转发数据包，使得交换机所连接的所有网络中断。

(4) 如果某一子网中存在着许多像路由器或者提供 NAT 服务的服务器这些具有 IP 转发功能的主机，利用 ARP 篡改的技术则可以实现多种形式的信息洪泛。假设某子网包含了具有 IP 转化功能的主机 1、2 和 3，通过 ARP 欺骗，把主机 1 的 ARP 缓存中默认网关对应的 MAC 地址改为主机 2 的 MAC 地址，利用同样的方法把主机 2 的 ARP 缓存的默认网关对应的 MAC 地址改为主机 3 的 MAC 地址，这样主机 1 到网关的数据通道就变成了 1—2—3—网关，如果 1 的数据流量很大，则 2、3 也会有较高的负荷，并且分析可知被欺骗后子网的通讯流量是原来的三倍。从而形成讯息洪泛，整个子网的性能就急剧降低了。

4.4 IP 地址冲突

进攻主机发送更改后的 ARP 报文，其包括目的主机的 IP 地址和伪装的 MAC 地址，当系统检测到两个不同的 MAC 地址对应同一个 IP 地址则会提示 IP 地址冲突，在 Windows 操作系统中弹出警告对话框，Unix/Linux 操作系统上表现为系统以 mail 方式警告用户,这两种情况下都会使目的主机发生网络中断。

4.5 克隆攻击

如今,攻击者已经能修改网络接口的 MAC 地址。攻击者首先对目标主机进行拒绝服务攻击,使其不能对外部做出任何反应。然后攻击者就可以将自己的 MAC 地址与 IP 地址分别改为目标主机的 MAC 地址与 IP 地址,这样攻击者的主机就变成了目标主机的副本，从而进一步伪装了自己更进一步的实施各种非法攻击,窃取各种通信数据[2]。

5 针对ARP协议漏洞的解决方案

提出基于 ARP 协议的进攻各种方式其最根本的就是利用主机对 ARP 应答的无条件的信任，篡改主机的 ARP 缓存，从而实现各种攻击。而且不同的 ARP 进攻有着不同的特征，在本小节中，结合网络管理的实际工作，针对不同的进攻方式将给出解决方案。

(1) 设置静态的 ARP 缓存表

ARP 协议进攻最根本的原理就是改变 IP 地址与 MAC 地址对应关系，所以可以通过设置静态的 ARP 缓存表来防止 ARP 协议攻击。设置静态 ARP 表有两种方法，一是在目的主机的 ARP 缓存中设置静态的地址映射记录，二是在三层交换机设置 IP-->MAC 地址对应表。在三层交换机上设置后，攻击主机就没有机会应答向其他主机发送 ARP 请求。如果攻击者在未收到 ARP 请求的情况下仍凭空伪造 ARP 应答请求发送给其他主机，三层交换机将拒绝用伪造的数据更新 ARP 缓存表中的静态记录。这种方法比较简单，比较直观，但是在经常要更换 IP 地址且有较多主机的的局域网里，这种方法就显得十分繁琐，工作量大。

(2) 交换机上绑定端口和 MAC 地址

交换机的每一个端口都对应着一台主机，而每一台主机的 MAC 都是唯一的。设置交换机的每一个端口与 MAC 地址相对应，如果来自该端口的 MAC 地址与之前的 MAC 地址不相符，就自动封锁该端口，使其不能连接到局域网。这样，进攻主机就无法发送伪造的 ARP 数据帧，从而有效的防止了 ARP 欺骗的发生。在交换机中，绑定端口和 MAC 地址通常用到 ACL 配置。访问控制列表(Access Control List，ACL)通过一系列的匹配条件对数据包进行分类，交换机根据 ACL 中指定的条件来检测数据包，从而决定是转发还是丢弃该数据包。下面我们结合一个实例来说明该问题。如下图，.三层华为交换机 S3536E Switch A 有两个端口 Ethernet 0/1、Ethernet 0/2 分别属于 vlan 1、vlan 2，vlan 1、vlan 2 的三层接口地址分别是 1.0.0.1/8、2.0.0.1/8。组网要求是静态 Mac、端口捆绑：端口

Ethernet 0/1 仅仅允许 pc1(Mac：1.1.1)接入。

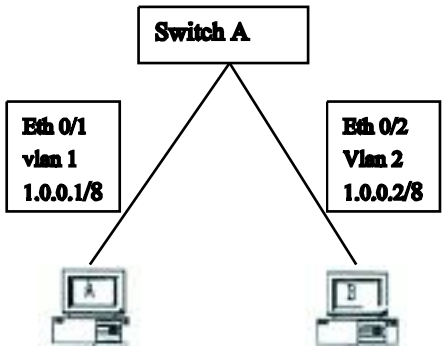

图 2　端口和 MAC 地址绑定

① 创建 ACL

[Switch A] ACL num 2000

② 定义规则禁止 E0/1 去往任意端口的数据包

[SwitchA-acl-link-200] rule 0 deny ingress interface e0/1 egress any

③ 定义规则允许 1.1.1 的 MAC 地址从 E0/1 发住任意端口

[SwitchA-acl-link-200] rules 1 permit ingress 1.1.1 interface e0/1 egress any

④ 下发访问控制列表

[Switch A] packet-filter link-group 2000

由上可知，当区域网要加入一台主机或者移除一台主机的时候都得手工配置，该方法虽然能够比较好的防止 ARP 病毒，但是缺点是不灵活。

(3) VLAN 技术

文献[3]提出为了减少 ARP 进攻,可以把网络分为多个子网。一般情况下，ARP 广播包是不能跨子网或者网段传播的，言下之意就是说子网、网段可以隔离广播包。一个 VLAN 就是一个逻辑广播域,通过 VLAN 技术可以在局域网中创建多个子网，就在局域网中隔离了广播，缩小了广播范围，也就减小了广播风暴的产生的几率。如果利用 VLAN 技术将相互信任的主机所在的安全子网与进攻者可能访问的不安全子网隔离开来，对不安全的子网中采用 ARP 静态记录。在安全的子网中，就可以采用最基本的方法发送 ARP 请求，安全子网的主机与不安全子网的主机通讯由三层交换机做“代理”，三层交换机采用静态记录来抵御来与不安全子网上进攻者实施的 ARP 进攻。从效果来看，就解决了上段最后提出的问题，即安全子网中的主机与不安全子网上的主机通信时，只相信来自于三层交换机(相当于 ARP 服务器)的 ARP 响应。而且划分过后的局域网，即使其中的一个 VLAN 受到 ARP 攻击后，也不影响其他 VLAN 主机的工作。同时 VLAN 的划分对于 ARP 病毒定位非常有帮助，能快速的定位受进攻的主机。

(4) 建立信任 IP－MAC 地址映射表

上面两种方法的不足之处都是需要手动的维护静态记录，工作比较分散。为了解决这个问题，可以在局域网内部指定一台主机作为 ARP 服务器来集中管理，用它来保存和维护局域网内相对可靠主机的 IP－MAC 地址映射记录。当局域网内有 ARP 请求时，服务器就通过查询自己的 ARP 缓存的静态记录并以被查询主机的名义响应 ARP 请求，并且服务器按照一定的时间间隔在局域网内广播正确的 IP－MAC 地址表。同时，设置局域网内部的其他主机只使用来自 ARP 服务器的 ARP 响应。这个方法看起来很完美，但是目前还很难将主机配置成只相信来自 ARP 服务器的 ARP 响应。文献[4]提出采用一种模糊逻辑方法可以区分正常和异常的 ARP 响应,设置后的模糊逻辑控制器可根据网络变化采用动态的方法把主机相关的信息存储到数据库,根据这些信息来判断 ARP 响应的可信度。在这介绍一种通过交换机实现对信任 IP 地址和 MAC 地址管理的方法，DHCP SNOOPING 即 DHCP 服务器的二层监听功能，在交换机上开启 DHCP SNOOPING 功能后，以太网交换机就可以通过监听 DHCPACK 或 DHCPREQUEST 报文，记录 DHCP 客户端 IP 地址与 MAC 地址的对应关系，通过设置 DHCP SNOOPING 信任端口，保证主机能从合法的服务器获取 IP 地址，从而实现了对不信任 DHCP 报文的过滤功能。这样进攻者将无法伪造 ARP 应答包，也不能通过 MAC 地址替换来达到嗅探的目的了。在这里要注意的是 DHCP Snooping 表只记录了通过 DHCP 方式动态获取 IP 地址的客户端信息。如果主机的 IP 地址固定的，必须在交换机上手工配置 IP 静态绑定表的表项，即要绑定用户的 IP 地址、MAC 地址及连接该用户的端口。

(5) ARP 报文限速

由广泛拒绝服务攻击 DOS 来看，ARP 欺骗还有一个特征就是不断的发送 ARP 欺骗包，以达到欺骗的目的。对于该类的广泛 DOS,我们可以通过设置三层交换机的 ARP 报文限速避免其进攻。ARP 报文限速就是限制端口接受 ARP 报文的单位时间的数量。当通过

交换机启动某个端口的 ARP 报文限速功能后,交换机会统计该端口每秒内接收的 ARP 报文数量,如果每秒内统计到的的 ARP 报文数量超过设定值,则认为该端受到 ARP 报文攻击。此时,交换机将关闭该端口,使其不再接收任何报文,经过一段时间自动恢复被关闭的端口的开启状态。从而避免大量 ARP 报文攻击设备。需要注意的是 ARP 包的速率限制要根据具体环境而设置,需要测试后才能实施。

6 ARP欺骗检测方法

目前主要存在 2 种检测 ARP 欺骗的机制。在主机级,普通主机可以采用两种方法检测自己的是否正在被其它主机欺骗:一种是主动探查可疑的主机;另一种是被动检查网络 ARP 广播报文。在网络级,处于网络管理员控制下的机器将检查所有的 ARP 请求与响应以查明异常并判断是否出现 ARP 欺骗行为[5]。

(1) 主机级检测方法

① 主动检测。当主机收到 ARP 应答报文时,从应答报文中提取 MAC 地址,然后构造一个 RARP 请求报文,这样就可以得到这个 MAC 地址对应的 IP 地址,比较两个 IP 地址,如果不同,就说明有主机进行了 ARP 欺骗。还有另外一种方法就是:主机定期向区域网发送查询自己 IP 地址的 ARP 请求报文。如果收到其它主机的应答,就说明该区域网可能存在 ARP 欺骗。

② 被动检测。当系统接收到来自局域网上的 ARP 请求时,系统检查该请求发送端的 IP 地址是否与自己的 IP 地址相同。如果相同,则说明该网络上另有一台机器与自己具有相同的 IP 地址[5]。当然还有一种情况,就是每当系统启动时或更改主机 IP 地址时,ARP 协议自动地向本地网络发送一个广播请求包,通告自己的 IP 地址并检测是否存在 IP 地址冲突。

由上可知,主机级检测出来的异常情况,可能是由于用户操作失误或者其它原因造成的,并不能有效和准确的检测出 ARP 欺骗,下面介绍的检测方法更能有效的检测出 ARP 欺骗。

(2) 网络级检测方法

① 通过配置主机定期向中心管理主机报告其 ARP 缓存的内容。这样中心管理主机上的程序就会查找出两台或者多台主机报告信息的不一致,以及同一台主机前后报告内容的变化[6]。根据这些情况可以初步确定谁是进攻者,谁被进攻者。这里需要考虑的是:每台主机向衷心管理主机发送数据的时间间隔,如果发送的间隔太短会占用通讯的信道,影响整个区域网通讯的性能,如果间隔太长,以至超过攻击者一次进攻的时间,进攻者可能在短时间内攻击之后又把一切都恢复了,则失去意义。

② 中心管理主机上保存着可信任的 IP/MAC 映射表,然后通过检查匹配网络的 IP/MAC 映射表,检测 ARP 欺骗。可信任的 IP/MAC 映射表可以有管理员手动配置,也可以在网络正常时通过 ARP 扫描获取网内的 IP/MAC 映射表。

7 结语

ARP 协议的安全缺陷来源于协议自身设计上的不足。本文详细的分析了 ARP 协议的工作原理和协议的漏洞,针对 ARP 协议的缺陷多方位的分析了 ARP 进攻的方式,针对不同的 ARP 进攻方式结合的实验结果给出抵御的方法。上述的各种防御措施和检测方法既有它本身的优点,也有各自的局限性,因而在实际处理过程中,针对不同情况需要应对不同的策略。

参考文献

1 王佳,李志蜀.基于 ARP 协议的攻击原理分析.微电子学与计算机, 2004,21(4):10－12.

2 王燕,张新刚.基于 ARP 协议的攻击及其防御方法分析.微计算机信息, 2007,23(12):72－74.

3 Cristina LA, Rafael IB. An analysis on the schemes for detecting and preventing ARP cache poisoning Attacks. Distributed Computing Systems Workshops, 2007. ICDCSW'07. 27th International Conference. 22－29 June 2007.

4 Trabelsi Z. El-Hajj. Preventing ARP Attacks Using a Fuzzy-Based Stateful ARP Cache. Communications, 2007. ICC'07. IEEE International Conference. 24－28 June 2007.

5 任侠,吕述望. ARP 协议欺骗原理分析与抵御方法.计算机工程, 2003,29(9):127－128.

6 郭卫兴,刘旭,吴灏.基于 ARP 缓存超时的中间人攻击监测方法.计算机工作, 2008,34(13):133－135.