校园网中 ARP 欺骗攻击及其防范①

ARP Spoofing Attack and Its Prevention in Campus Network

王胜和 (安徽公安职业学院 公安科技系 安徽 合肥 230031)

摘 要： 目前 ARP 欺骗攻击呈现出越来越严重的趋势，已成为导致校园网大面积断网甚至瘫痪的首要原因。针对校园网中屡屡发现的 ARP 欺骗攻击，分析其攻击原理、症状，并提出了切实可行的解决方法和防范策略。

关键词： 地址解析协议 ARP 欺骗攻击 网络安全 校园网

近期，一种新型的“ ARP 欺骗”木马病毒正在校园网中扩散，严重影响了校园网的正常运行。ARP 欺骗木马的中毒现象表现为：使用校园网时会突然掉线，过一段时间后可能恢复正常，通过重启机器或在 MS-DOS 窗口下运行命令“arp－d”后，又可恢复上网。ARP 欺骗木马十分猖狂，危害也特别大，各大学校园网、小区网、公司网和网吧等局域网都出现了不同程度的灾情。ARP 欺骗木马只需成功感染一台电脑，就可能导致整个局域网都无法上网，严重的甚至可能导致整个网络的瘫痪。该木马发作时除了会导致同一局域网内的其他用户上网出现时断时续的现象外，还会窃取用户密码，如盗取 QQ 密码、盗取各种网络游戏密码和账号、盗窃网上银行账号做非法交易活动等，这是木马的惯用伎俩，给用户造成了很大的不便，甚至带来经济损失。

1 ARP欺骗攻击原理

在 TCP/IP 网络环境下，一个 IP 数据包到达目的地所经过的网络路径是由路由器根据数据包的目的 IP 地址查找路由表决定的，但 IP 地址只是主机在网络层中的地址，要在实际的物理链路上传送数据包，还需要将 IP 数据包封装到 MAC 帧后才能发送到网络中。同一链路上的哪台主机接收这个 MAC 帧是依据该 MAC 帧中的目的 MAC 地址来识别的，即除了同一链路上将网卡置为混杂模式的主机外，只有当某台主机的 MAC 地址和链路中传输的 MAC 帧的目的 MAC 地址相同时，该主机才会接收这个 MAC 帧并拆封为 IP 数据包交给上层模块处理。因此，每一台主机在发送链路层数据帧前都需要知道同一链路上接收方的 MAC 地址，地址解析协议 ARP 正是用来实现 IP 地址到 MAC 地址的转换的。同时为了避免不必要的 ARP 报文查询，每台主机的操作系统都维护着一个 ARP 高速缓存，记录着同一链路上其它主机的 IP 地址和 MAC 地址的映射关系。ARP 协议虽然是一个高效的数据链路层协议，但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，所以 ARP 协议存在以下缺陷：ARP 高速缓存根据所接收到的 ARP 协议包随时进行动态更新；ARP 协议没有连接的概念，任意主机即使在没有 ARP 请求的时候也可以做出应答；ARP 协议没有认证机制，只要接收到的协议包是有效的，主机就无条件的根据协议包的内容刷新本机 ARP 缓存，并不检查该协议包的合法性。因此攻击者可以随时发送虚假 ARP 包更新被攻击主机上的 ARP 缓存，进行地址欺骗或拒绝服务攻击。

针对交换机根据目的 MAC 地址来决定数据包转发端口的特点，ARP 欺骗攻击的实现一般原理为[1]：假设主机 C 为实施 ARP 欺骗的攻击者，其目的是截获主机 B 和主机 A 之间的通信数据，且主机 C 在实施 ARP 欺骗前已经预先知道 A 和 B 的 IP 地址。这时 C 先发送 ARP 包获得主机 B 的 MAC 地址，然后向 B 发送 ARP Reply 数据包，其中源 IP 地址为 A 的 IP 地址，但是源 MAC 地址却是主机 C 的 MAC 地址。主机 B

① 收稿时间:2008-12-24

收到该 ARP Reply 后，将根据新的 IP 地址与 MAC 映射对更新 ARP 缓存。这以后当 B 给 A 发送数据包时，目标 MAC 地址将使用 C 的 MAC 地址，因此交换机根据 C 的 MAC 地址就将数据包转发到攻击者 C 所在的端口。同理，攻击者 C 发送 ARP Reply 使主机 A 确信主机 B 的 MAC 地址为 C 的 MAC 地址。在间歇的发送虚假 ARP Reply 的同时，攻击者 C 打开本地主机的路由功能，将被劫持的数据包转发到正确的目的主机，这时攻击者对主机 A 和 B 来说是完全透明的，通信不会出现异常，但实际上数据包却被 C 非法截获，攻击者 C 成为了“中间人”。 从 ARP 欺骗的实现原理看,ARP 欺骗分为两种形式：第一种是截获网关数据。它通知网关一系列错误的内网 MAC 地址，并按照一定的频率不断进行，使真实的地址信息无法通过更新保存在网关的路由中，结果网关的所有数据只能发送给错误的 MAC 地址，造成正常 PC 无法收到信息，或信息被监听转发。第二种是伪造网关。它是建立假网关，让被它欺骗的 PC 向假网关发数据，而不是通过正常的网关途径上网，造成 PC 无法上网。

2　ARP欺骗攻击检测

为了确认机器受到了 ARP 欺骗攻击，可以采用以下方法检测：

(1) 在命令行状态下使用 ARP -A 命令，来查看本机的 ARP 缓存状态。正常情况下除了网关外不会有其它记录，需要查看网关的 MAC 地址是否和正常的一样。如果不同，那么或者网关换了网卡，或者受到了 ARP 欺骗的攻击。如果没有记录或者有过多的 ARP 记录，则也可能受到了攻击。

(2) ping 网关，看是否连接正常。如果 ping 网关不通或丢几个包，然后又连上，则可能受到了攻击。

(3) 使用 arp -d 命令，看看能否恢复上网。使用 arp -d 命令后，若可暂时恢复上网，说明已删除 ARP 缓存表，恢复了默认 ARP 缓存表。

(4) 运行路由跟踪命令 tracert。正常情况是 tracert 执行后的输出第一跳应该是默认网关 IP 地址，若发现第一跳不是网关的 IP，而是本网段内的另外一台机器的 IP，再下一跳才是网关的内网 IP，由此判定第一跳的那个非网关 IP 地址的主机就是罪魁祸首。

3　ARP欺骗攻击解决思路[2]

(1) 不能仅仅把网络安全信任关系建立在 IP 基础上或 MAC 基础上(RARP 同样存在欺骗的问题)，理想的关系应该建立在 IP 和 MAC 基础上。

(2) 设置静态的 MAC—IP 对应表，不让主机刷新设定好的转换表。

(3) 使用 ARP 服务器，通过该服务器查找自己的 ARP 转换表来响应其他机器的 ARP 广播。

(4) 使用 Proxy 代理 IP 的传输。

(5) 使用硬件屏蔽主机,设置好路由，确保 IP 地址能到达合法的路径(静态配置 ARP 路由表)。

(6) 管理员定期轮询，检查主机上的 ARP 缓存。

(7) 使用 ARP 防火墙连续监控网络,一旦发现有 ARP 欺骗攻击,立即寻根究源,及时阻断攻击机器。

4　ARP欺骗攻击防御方案

在上述解决思路的指导下还需根据网络软硬件的实际情况制定切实可行的方法。

4.1 网络设备不具备网管功能的解决方案

此方案对一般规模较小的网络适用，处理方法是：

(1) 对全网络中的所有计算机进行一次彻底的杀毒处理,而且还得保证日后没有计算机感染 ARP 病毒，这样才能免受 ARP 病毒的苦恼；

(2) 在网络中安装网络版的 ARP 病毒防火墙，控制网内 ARP 病毒的发作；

(3) 对网络中的所有机器进行 IP—MAC 地址绑定，并把使用人、IP 地址、MAC 地址登记备案，以便发现 ARP 攻击时快速定位追踪到攻击源。

4.2 网络设备具备网管功能，能进行规则配置和地址绑定

此方案对大规模网络，并且网络结构复杂的网络比较适用，但工作量是很庞大的。参见文献[3,4]，处理方法是：

4.2.1 防止仿造网关 IP 的攻击

(1) 对于二层交换机的配置

网络结构如图 1 所示(以华为 S 系列交换机为例):

S3552P 是三层交换机，其中 IP: 100.1.1.1 是所有 PC 的网关，S3552P 上的网关 MAC 地址为 000f-e200-3999。假定 PC-B 上有 ARP 欺骗攻击，现在需要对 S3026_A 进行一些特殊配置，目的是过滤掉仿冒网关 IP 的 ARP 报文。对于二层交换机如 S3026C 等支持用户自定义 ACL(number 为 5000 到 5999)的交换机,可以配置 ACL 来进行 ARP 报文过滤，禁止所有源 IP 是网关的 ARP 报文。

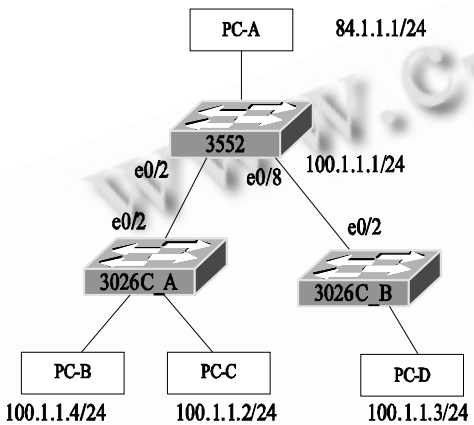

图 1　二层交换机配置组网

先全局配置 deny 所有源 IP 是网关的 ARP 报文(自定义规则):

acl num 5000

rule0 deny 0806 ffff 24 64010101 ffffffff 40

rule1 permit 0806 ffff 24 000fe2003999 ffffffffffff 34

其中，rule0 把整个 S3026C_A 的端口冒充网关的 ARP 报文禁掉，其中 64010101 是网关 IP 地址 100.1.1.1 的 16 进制表示形式。Rule1 把上行口的网关发送的 ARP 报文允许通过，000fe2003999 为网关的 MAC 地址。

然后在 S3026C-A 系统视图下配置 ACL 规则:

[S3026C-A] packet-filter user-group 5000

这样只有 S3026C_A 上连网关设备才能够发送网关的 ARP 报文，其它主机都不能发送假冒网关的 ARP 响应报文。

(2) 对于三层交换机的配置

网络结构如图 2 所示:

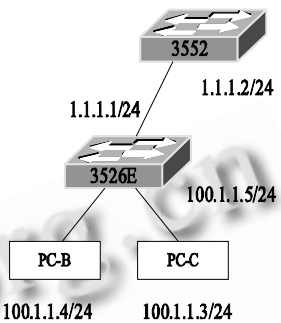

图 2　三层交换机配置组网

对于三层设备，需要配置过滤源 IP 是网关的 ARP 报文的 ACL 规则，配置如下 ACL 规则:

acl number 5000

rule0 deny 0806 ffff 24 64010105 ffffffff 40

rule0 禁止 S3526E 的所有端口接收冒充网关的 ARP 报文,其中 64010105 是网关 IP 地址 100.1.1.5 的 16 进制表示形式。

4.2.2 仿冒他人 IP 的 ARP 攻击

作为网关的设备有可能会出现 ARP 错误表项，因此在网关设备上还需对仿冒他人 IP 的 ARP 攻击报文进行过滤。

网络结构如图 1 所示，当 PC-B 发送源 IP 地址为 PC-D 的 ARPreply 攻击报文，源 MAC 是 PC-B 的 MAC(000d-88f8-09fa)，源 IP 是 PC-D 的 IP(100.1.1.3)，目的 IP 和 MAC 是网关(3552P)的，这样 S3552 上就会学习错误的 ARP，如下所示:

---------- 错误 ARP 表项 ----------

IP Address MAC Address VLANID Portname Aging Type

100.1.1.4 000d-88f8-09fa 1 Ethernet0/2 20 Dynamic

100.1.1.3 000f-3d81-45b4 1 Ethernet0/2 20 Dynamic

从网络连接可以看出 PC-D 的 ARP 表项应该学习

到端口 E0/8 上，而不应该学习到 E0/2 端口上。但实际上交换机上学习到该 ARP 表项在 E0/2。通过如下配置方法可以防止这类 ARP 的攻击。

(1) 在三层设备(S3552)上配置静态 ARP，可以防止该现象：

arp static 100.1.1.3 000f-3d81-45b4 1 e0/8

(2) 对于二层设备(S3026C)，除了可以配置静态 ARP 外，还可以配置 IP+MAC+PORT 绑定，比如在 S3026C 端口 E0/4 上做如下操作：

am user-bind ip-addr 100.1.1.4 mac-addr 000d-88f8-09fa int e0/4

则 IP 为 100.1.1.4 并且 MAC 为 000d-88f8-09fa 的 ARP 报文可以通过 E0/4 端口，仿冒其它设备的 ARP 报文则无法通过，从而不会出现错误 ARP 表项。

上述配置案例中仅仅列举了部分华为 S 系列以太网交换机的应用。在实际的网络应用中，可根据配置手册确认该产品是否支持用户自定义 ACL 和地址绑定，仅仅具有上述功能的交换机才能防止 ARP 欺骗。

5 结语

ARP 协议的安全缺陷来源于协议自身设计上的不足。本文对 ARP 协议的工作原理、安全缺陷进行了分析，分析了基于 ARP 协议安全缺陷的攻击，并提出了相应的防御方案。这些方案能有效抵御 ARP 欺骗攻击，但管理维护的工作量还是相当大的。要想彻底解决 ARP 欺骗攻击，最根本的措施就是使用 IPv6 协议，因为在 IPv6 协议定义了邻机发现协议(NDP)，把 ARP 纳入 NDP 并运行于因特网控制报文协议(ICMP)上，使 ARP 更具有一般性，包括更多的内容，而且不用为每种链路层协议定义一种 ARP。NDP 中还定义了可达性检测过程，保证 IP 报文不会发送给“黑洞”。

参考文献

1 谭思亮.监听与隐藏-网络侦听揭密与数据保护技术.北京:人民邮电出版社,2002:202－208

2 白晓梅.局域中 ARP 欺骗攻击解决方案.鞍山师范学院学报, 2007,9(6):56－57.

3 http://blog.tom.com/dgt110/article/.

4 石硕,林莉,杨签,杨玲.交换机/路由器及其配置.北京:电子工业出版社,2003:145－148