

园区网中 ARP 欺骗防范设计与实现

夏栋梁 廖梦怡

(平顶山学院,平顶山 467000)

摘 要 ARP 欺骗对园区网的正常使用造成了很大的影响。阐述了 ARP 欺骗的原理和常见的欺骗类型,并提出了解决方案。通过交换机的端口安全、ARP – Check 等功能和 GSN® 机制防止 ARP 欺骗,实际应用效果良好。

关键词 ARP 欺骗 MAC 地址 交换机 GSN 机制

中图法分类号 TP393.8; **文献标志码** A

近来,许多园区网中都出现了 ARP 攻击现象,给园区网的正常使用造成了很大的影响,甚至造成园区网中大量用户无法访问外部网络。同时,ARP 病毒清理和防范都相对比较困难,给许多网络管理员造成了很大的困扰,所以我们很有必要分析一下 ARP 欺骗的原理。

1 ARP 欺骗的原理及类型

ARP(Address Resolution Protocol,地址解析协议)是一个位于 TCP/IP 协议栈中的底层协议,对应于数据链路层,负责将某个 IP 地址解析成对应的 MAC 地址^[1]。

当计算机接收到 ARP 应答数据包的时候,就会对本地的 ARP 缓存进行更新,将应答中的 IP 和 MAC 地址存储在 ARP 缓存中。协议设计者当初并没有考虑,ARP 协议不只在发送了 ARP 请求才接收 ARP 应答。如果网络中,某台设备发送一个伪造的 ARP 应答,网络就可能出现问题。

1.1 ARP 欺骗原理^[2]

假设某小型局域网中,有三台主机 PC1、PC2、PC3。PC1 的地址为:IP:192.168.1.1,MAC: 00-1F-D0-58-EF-D1; PC2 的地址为: IP: 192.168.1.2,

MAC: 00-1F-D0-58-EF-C3 ;PC3 的地址为:IP:192.168.1.3,MAC: 00-1F-D0-58-E6-D6。如图 1 所示。

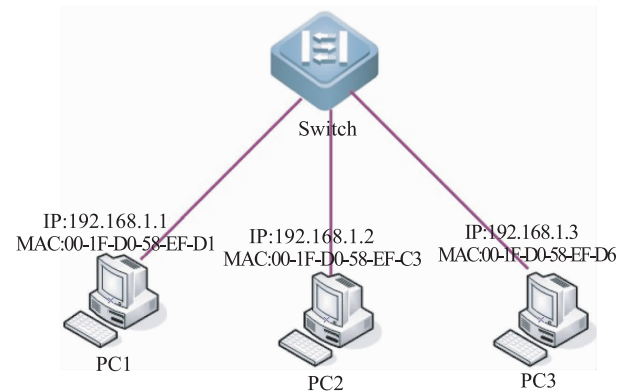


图 1 局域网结构图

正常情况下 PC1 和 PC3 之间进行通讯,但此时 PC2 向 PC1 发送一个自己伪造的 ARP 应答,而这个应答中的数据为发送方 IP 地址是 192.168.1.3 (PC3 的 IP 地址),MAC 地址是 00-1F-D0-58-EF-C3 (PC3 的 MAC 地址本来是 00-1F-D0-58-E6-D6)。当 PC1 接收到 PC2 伪造的 ARP 应答后,就会更新本地的 ARP 缓存,这时 PC2 就伪装成为了 PC3,PC1 被欺骗了。同理,PC2 可以向 PC1 发送一个 ARP 应答,伪装成为 PC3。这就是典型的 ARP 欺骗过程。

1.2 ARP 欺骗类型

1.2.1 网关欺骗

网络中,攻击者通过伪造 arp request/reply 报文,在报文的源 IP 地址字段中填入网关的 IP 地址,但源 MAC 地址不是网关 MAC 地址,一般情况下为

2011 年 6 月 20 日收到
第一作者简介:夏栋梁(1981—),男,河南鄢陵人,硕士,助教,研究方向:网络安全、网络工程,等。E-mail:xdllhero@163.com。

发起攻击者的主机 MAC 地址。从而导致其它客户端更新主机的 ARP 缓存表,形成错误的对应关系。网络中,到网关的通信的数据包都被转发到了发起攻击的主机上^[3]。

1. 2. 2 协议报文欺骗

攻击者通过伪造 arp request/reply 报文,在报文源 IP 地址或源 MAC 地址字段填入非法的 IP 地址或 MAC 地址,导致其它主机或网关更新 ARP 缓存表,形成错误的对应关系^[4]。

1. 2. 3 ARP 报头欺骗

攻击者通过伪造 ARP 报头字段,在数据帧源 MAC 地址字段中填入网关的 MAC 地址,导致交换机中的 MAC 地址表形成错误的对应关系,无法正常转发数据帧,同时可能向外发出大量的广播报文^[5],导致网络拥塞,使得主机无法与网关及其他主机正常通信。

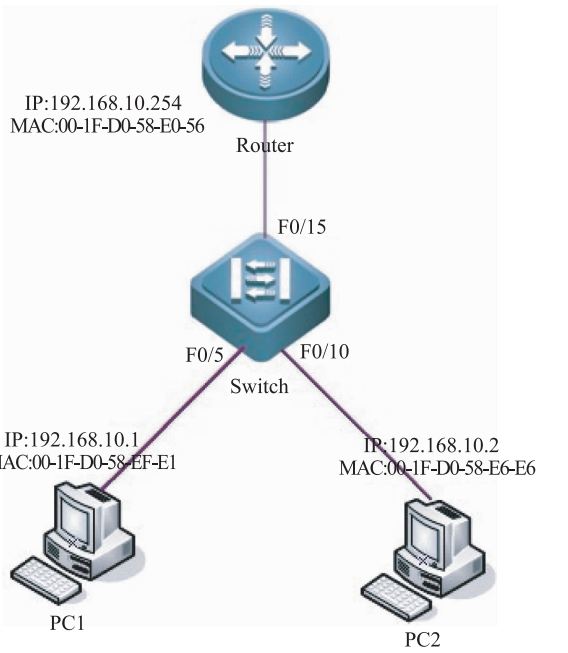


图 2 网络结构图

2 防止 ARP 欺骗的解决方案

2.1 利用交换机防止 ARP 欺骗

在交换机上,通过配置防止 ARP 欺骗。本文将通过一个实例进行分析。假设用户 PC1 的 IP 为 192.168.10.1,攻击者 PC2 的 IP 为 192.168.10.2,网关的 IP 为 192.168.10.254,对攻击者 PC2 的网关欺骗进行防御。如图 2 所示。

2. 1. 1 anti-arp-spoofing

在交换机接口模式下开启 anti-arp-spoofing 功能,防止 ARP 欺骗。在交换机上做如下配置:

```
Switch (config) #interface fastEthernet 0/10
Switch (config-if) #Anti-ARP-Spoofing ip 192.168.10.254 //过滤 arp 协议报文中,源 IP 为指定 IP 192.168.10.254 的 arp 报文
```

2. 1. 2 端口安全和 ARP-Check

利用交换机的端口安全和 ARP - Check 组合功能防止 ARP 攻击。

① PC 机使用静态 IP 地址是,在交换机上做如下配置:

```
Switch (config) #port-security arp-check //启动 arp-check 功能
Switch (config) #interface fastEthernet 0/10
Switch (config-if) #switchport port-security //打开端口安全功能
```

```
Switch (config-if) #switchport port-security maximum 1 //配置最大安全地址数
Switch (config-if) #switchport port-security mac-address 001f. d058. efe1
ip-address 192.168.10.2 //静态绑定安全 IP 地址及 MAC 地址
```

② 当 PC 机从 DHCP 服务器获取动态 IP 地址时,在交换机上做如下配置:

```
Switch (config) #service dhcp //打开 DHCP 中继功能
Switch (config) #service dhcp address - bind port //动态绑定 DHCP 分配的 IP 地址
```

需要指出的是,动态绑定仅适用于所绑定的 IP 及 MAC 数与端口安全最大地址数一致的情况,当端口安全最大地址数大于所绑定的 IP 及 MAC 数时,是无法避免攻击者伪造 ARP 攻击报文的。

2. 1. 3 MAC ACL + Arp - check + MAC 地址绑定

当主机 PC2 利用 sniffer 攻击时,通过 Mac ACL、ARP - check 和 Mac 地址绑定组合功能,防止 Arp 攻击。在交换机做如下配置:

```
Switch# (config) Mac access - list extended macarp //定义一个 MAC 地址访问控制列表并且命名为 macarp
Switch (config) #deny host 001f. d058. efe1 any //定义主机 PC1 可以访问任意主机
Switch (config) permit any any //定义所有主机可以访问主机 PC1
```

```
Switch(config-if) mac access-group test in
```

2.2 利用 GSN® 机制防止 ARP 欺骗

千兆字节系统网络(Gigabyte System Network 简称 GSN)是带宽最宽、延迟时间最小的互连网络标准。GSN® 由锐捷安全交换机、安全客户端、安全管理平台、用户认证系统、安全修复系统、VPN 客户端、RG - WALL 防火墙等多重网络元素组成,实现同一网络环境下的全局联动,使网络中的每个设备都在发挥着安全防护的作用,构成的全新安全体系。

GSN 从 ARP 协议自身的特点入手,在客户端进行静态 ARP 的绑定,在网关进行可信任 ARP 绑定,以达到从根本上解决 ARP 欺骗的问题。

2.2.1 主机 ARP 静态绑定

首先在主机上进行网关的 ARP 静态绑定,使用静态绑定方式,从而防止主机受到其它主机的 ARP 网关欺骗。当用户上线时,SMP 下发该用户所对应的网关 IP 和 Mac 地址,由 SU 在主机端进行网关 Mac 和 IP 的 ARP 静态绑定。SU 在认证成功后进行 ARP 静态绑定,然后定时进行 ARP 静态绑定是否被更改的检测,如果被更改,则重新进行绑定,以防止一些病毒或木马以合法的方式对 ARP 静态绑定进行的修改。当用户下线时,系统自动删除主机的网关 ARP 静态绑定。如图 3 所示。

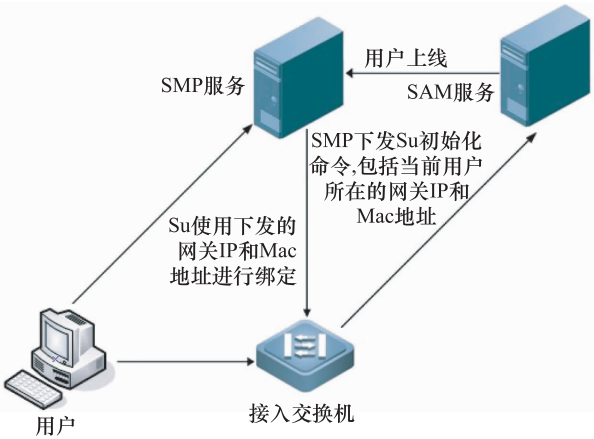


图 3 主机 ARP 静态绑定流程

2.2.2 防止主机冒充其他主机欺骗网关

当用户上线时,由 SAM 传递用户的网关信息,SMP 根据网关的相关信息,在网关完成主机 IP 地址

和 Mac 地址的 ARP 静态绑定。把该方式与主机 ARP 静态绑定结合起来使用,能够达到双绑定的效果。用户上线时,通过 SMP 在网关进行可信任 ARP 的绑定,当用户下线时,通过 SMP 在网关删除可信任的 ARP。如图 4 所示。

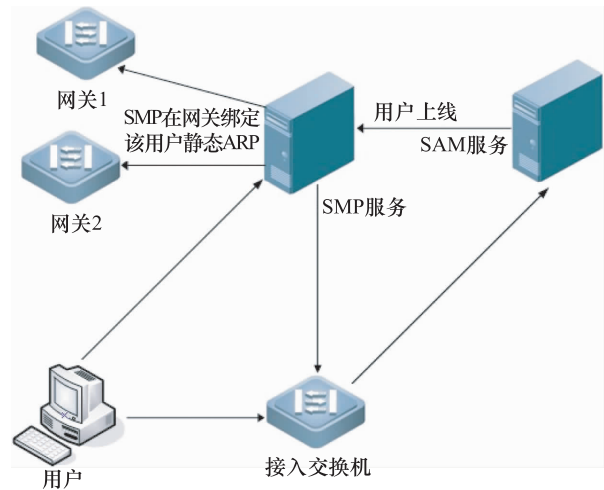


图 4 网关可信任绑定流程

总之,通过主机静态 ARP 绑定和网关可信任 ARP 绑定,能够彻底解决网络中存在的主机欺骗网关和主机欺骗其他主机的 ARP 欺骗攻击行为。并且系统能够自动进行 ARP 绑定,实现自动防御。配置完成后,管理员不需要再进行手动的干预,大大降低了网络管理的复杂度。

3 结语

ARP 协议在设计上是存在一定缺陷的,黑客们可以利用这些漏洞发起攻击。本文简单介绍了 ARP 欺骗的原理和常见的攻击形式,详细介绍了在园区网中,防止 ARP 攻击的解决方案,实践证明,该解决方案可以有效地避免 ARP 欺骗发生,避免 ARP 攻击对园区网带来的影响。

参 考 文 献

1 谢希仁. 计算机网络(第 5 版). 北京:电子工业出版社, 2009
2 王继龙,安淑梅,邵 丹. 局域网安全实践教程. 北京:清华大学出版社, 2009
3 潘 风. 局域网中的 ARP 欺骗防范. 计算机时代,2007;(5):

28—29

5 黄睿达. 校园中 ARP 病毒原理和防范措施. 软件导刊,2010;(03):118—119

4 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;9:127—128

Design and Realization of the ARP Cheat Preventio in Campus Network

XIA Dong-liang, LIAO Meng-yi
(Pingdingshan University, Pingdingshan 467000, P. R. China)

[Abstract] the ARP cheat does harm to the normal function of the campus network. The principle and the common types of the ARP cheat are illustrated, and presented solutions. ARP cheat could be prevented by the port security of switches, functions such as ARP-Cheat and GSN® mechanism, which results in good practical effect.

[Key words] ARP cheat MAC address switch GSN mechanism



(上接第 6470 页)

4 吴君辉,殷肖川,张 薇. 基于模糊关联规则挖掘改进算法的 IDS 研究. 计算机测量与控制,2009;17(11):2256—2259

6 亢海力,王来生,蔡永旺. 基于概率的模糊加权关联规则挖掘. 计算机应用,2006;26(6):113—114

5 陆建江,徐宝文,邹晓峰. 模糊规则发现算法研究. 东南大学学报(自然科学版),2003;33(3):272—274

7 哈罗德,刘文红 编. Java 语言与 XML 处理教程:SAX, DOM, JDOM, JAXP 与 TrAX 指南. 北京:电子工业出版社,2003

A Fuzzy Association Rules Algorithm for XML Document

ZHU Xing-tong, XU Bo
(School of Computer and Electronics Information, Guangdong University of Petrochemical Technology, Maoming 525000, P. R. China)

[Abstract] With the emergence of a large number of XML data, the field of data mining raises new challenges. Traditional data mining algorithm is oriented relational database and data warehouse, and can not be directly used for data mining in XML documents. From the basic theory of fuzzy sets, by defining the softening properties of the domain partition boundary, a fuzzy association rules oriented XML data mining is proposed, and implement it used the Java language. Experimental results show that the algorithm is correct.

[Key words] XML documents data mining fuzzy association rules