一种改进的 ARP 协议欺骗检测方法

张 洁 武 装 陆 倜
(北京信息科技大学 北京 100085)

摘 要 ARP 协议欺骗作为一种交换式局域网中获取数据信息的方法,当用作攻击手段时,给网络安全带来了严重威胁。本文通过分析 ARP 协议的漏洞及 ARP 欺骗的原理,设计并实现了一种基于 IP 地址和物理地址标准对应库的 ARP 欺骗检测方法,达到了及时有效地检测出网络中存在的 ARP 欺骗报文的目的,实测表明效果良好,具有实用价值。

关键词 ARP 协议,ARP 欺骗,检测

A Checking Method of ARP Spoofing

ZHANG Jie WU Zhuang LU Ti
(Beijing Information Science & Technology University, Beijing 100085)

Abstract When ARP spoofing is used as an attack mean, it brings serious threats to the security of LAN. This paper analyzes the defects of ARP protocol and the basic principle of ARP spoofing. A method is designed and accomplished to monitor ARP spoofing packets, and this method is based on a standard corresponding database of IP address and MAC address. The testing of this method shows that it can work effectively and has a practical value.

Keywords ARP protocol, ARP spoofing, Checking method

1 引言

ARP 欺骗,即利用 ARP 协议的漏洞,通过向目标主机发送虚假 ARP 报文,来实现监听或截获目标主机通信数据的一种手段。但一旦将 ARP 欺骗用作非法目的,则会对网络用户及网络运行产生影响和破坏,如一些具有 ARP 欺骗功能木马病毒,不仅盗取网络用户的账户、密码等重要信息,还通过发送大量虚假 ARP 报文,使用户在上网过程中频繁掉线,造成网络的拥塞甚至大面积的网络瘫痪等,对网络的管理及其安全的维护提出了严峻的考验。

本文通过剖析 ARP 欺骗的原理,并针对 ARP 欺骗报文的特点,设计实现了一种有效检测 ARP 欺骗报文的方法。文中具体描述了该方法的设计原理及实现步骤等。

2 ARP 协议欺骗

ARP 地址解析协议[1](Address Resolution Protocol)的功能就是在 IP 地址和硬件地址(MAC 地址)间提供动态映射,使网络节点间通信的数据帧能够在链路中正确传输。

2.1 ARP 协议的漏洞

ARP 协议的实现,是建立在网络中各主机相互信任的基础上的,且保证了 ARP 协议的高效运行。但其协议本身却存在漏洞:首先,ARP 高速缓存表通常是动态更新的。源主机并不是每一次在发送数据前都广播 ARP 请求报文,而是先查找高速缓存中的地址映射表,且该表中的每条地址映射关系都设有超时限制,它只保存最近的地址对应关系。其次,ARP 协议是无状态的。即使没有发送 ARP 请求报文,主机也可以接收 ARP 应答,并且,只要该应答是有效的,主机就会刷新其高速缓存表。这样,攻击主机就可以随时向目标主机发送虚假 ARP 应答报文,篡改其缓存表中的地址映射关系,进而截获其通信数据。

2.2 ARP 欺骗的原理

根据欺骗对象的不同,ARP 欺骗可以分为两种形式:假冒主机的 ARP 欺骗,主要截获同网段中不同主机间的通信数据;假冒网关的 ARP 欺骗,主要截获内网主机与外网的通信数据。其基本原理为:攻击主机 C 分别向通信主机 A 和 B 发送伪造的 ARP 应答报文。其中,发送给主机 A 的 ARP 应答报文中的地址对应关系为"MAC C——IP B",发送给主机 B 的 ARP 应答报文中的地址对应关系为"MAC C——IP A"。主机 A 和 B 收到应答报文后,分别更新其缓存。当主机 A 和 B 再相互发送数据时,实际上均发送到了主机 C。此时,为了不中断主机 A 和 B 之间的通信,主机 C 还需要将截获到的数据再转发给双方。另外,由于 ARP 缓存的超时限制,主机 A 和 B 还会定期广播 ARP 请求,寻求对方的 MAC 地址。为了防止其 ARP 缓存被正确更新,主机 C 也要以一定的时间间隔不断地向两者发送虚假 ARP 应答。至此,主机 C 以"中间人"的身份,成功地监听到主机 A 和 B 之间的通信数据。

3 ARP 欺骗防范方法分析

由于 ARP 欺骗是基于网络协议自身缺陷而产生的,只要运行 ARP 协议的地方就会存在一定的安全隐患,但仍可以通过采取一些防范措施,来尽量避免 ARP 欺骗,或将其造成的破坏影响限制在最小范围内。目前有关 ARP 欺骗的防范方法主要分为两类:

(1)改进 ARP 协议。由于 ARP 协议本身缺陷而引起的安全问题,最根本的解决办法还是从协议自身出发,通过对协议运行机制的改进,弥补协议的漏洞。改进主要是针对 ARP 协议"无状态"的特点,其算法思想为:对接收到的 ARP 请求,不更新缓存表;只接收有发送请求的 ARP 应答报文,其它的都丢弃。该方法主要是针对单个的主机系统,修改其内核的 TCP/IP 函数源代码或编写底层驱动程序实现中间件。改进

张 浩 硕士研究生;武 装 副教授,硕士研究生导师;陆 倜 教授。

协议的方法虽然能有效防范 ARP 欺骗，但由于采用了复杂的数据结构，且需要对 ARP 应答报文进行更多的处理，使得改进后的协议运行效率降低。因此，无论上述哪种方式，实现代价都较大，在实际的应用中也存在较大的局限性。

(2)ARP 欺骗检测服务器。其实现原理为：该服务器获取网段中的所有 ARP 应答报文，并假设这些报文是 ARP 欺骗报文，提取应答报文中的源 IP 地址后，服务器向该 IP 地址主机发送 ARP 请求，将得到的正确 MAC 地址与原应答报文中的 MAC 地址比较。若不一致，则原应答报文存在欺骗。当检测到欺骗应答报文后，服务器向被欺骗的主机发送正确的 ARP 应答，以恢复其缓存中的 IP-MAC 地址对应关系。但是，当网络中存在 ARP 攻击时，会出现大量 ARP 欺骗应答报文，并造成网络拥塞，如果采用上述的恢复机制，对每个欺骗报文都发送正确的 ARP 应答，只会加重网络负担，并且服务器在检验应答报文真实性时，也采取了主动发送 ARP 请求的方法，增加了一定的网络负载。

4 ARP 欺骗检测方法

本文主要对上述第二种方法进行了改进，设计并实现了一种基于交换机镜像端口的 ARP 欺骗检测方法，其基本原理为：将运行 ARP 欺骗检测功能进程的主机连接到交换机的镜像端口，该镜像端口复制了其他被检测端口的进出口数据，检测主机过滤并分析这些数据中的所有 ARP 报文的 IP-MAC 地址对应关系，通过与标准关系库进行一致性对比，及时发现网络中的 ARP 欺骗报文。其流程如图 1 所示。

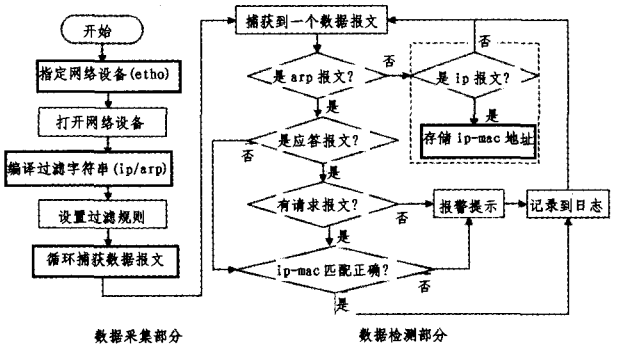

图 1 ARP 欺骗检测流程图

该方法首先摒弃了对 ARP 欺骗的恢复功能，重点为对欺骗的检测和对攻击主机的 MAC 地址锁定。该方法通过与事先建立的正确 IP-MAC 地址对应关系库匹配，来发现欺骗报文，而不用主动发送请求报文，完全为被动检测，不会对网络产生任何负载。另外，在理想的情况下，如果攻击主机不在欺骗报文中伪造自己的 MAC 地址，则可以在检测到其真实 MAC 后，再结合其它 IP 扫描工具(如 NetScan 等)锁定攻击主机，找出 ARP 欺骗的根源。

4.1 检测方法具体介绍

整个 ARP 欺骗监测过程分为三部分：ARP 数据报采集、IP-MAC 地址标准库建立、ARP 欺骗报文检测：

(1)ARP 数据报采集(图 1)

本文采用 Libpcap 开发库采集所需的数据报文。其采用 BPF(Berkeley Packet Filter)过滤机制，数据报捕获实现如下：

①指定“eth0”为数据采集的网络设备接口，该接口与交换机镜像端口相连。

net_interface = “eth0”;

②打开网络接口设备“eth0”，进行数据报文捕获，其中 BUFSIZE 定义捕获的报文长度，接口打开模式为混杂模式“1”，等待时间“0”，error_content 存储错误信息。

```
pcap_t * pcap_handle = pcap_open_live
(net_interface,BUFSIZ,1,0,error_content);
```

③编译 BPF 的过滤规则。其中“bpf_filter_string”设置为“ip or arp”。

```
pcap_compile(pcap_handle, & bpf_filter,
bpf_filter_string, 0 , net_ip);
```

④设置过滤规则。

```
pcap_setfilter(pcap_handle,&bpf_filter);
```

⑤循环捕获数据报文，并返回数据报文内容，调用 ehternet_vlan_switch_callback 函数对报文进行分析处理。

```
pcap_loop(pcap_handle,-1,
ethernet_vlan_switch_callback,NULL);
```

⑥关闭 Libpcap 操作句柄“pcap_handle”，结束报文捕获。

```
pcap_close(pcap_handle);
```

(2)IP-MAC 地址标准库建立(图 1 虚线部分)

IP-MAC 地址对应关系库是检测 ARP 欺骗报文的重要依据，其建立过程可以用两种方法实现：手工添加 IP-MAC 地址对应关系；或者通过解析数据的以太帧首部源 MAC 地址和 IP 数据报首部的源 IP 地址，动态添加地址对应关系，并不断学习完善。

(3)ARP 欺骗报文检测(图 1)

①当采集到 ARP 请求报文时，提取数据报中的源 IP 地址和源 MAC 地址，查找地址关系库。若有该地址对应关系，将该报文信息存储到日志文件，分析下一条报文；若无该地址对应关系，标记该日志记录，报警提示。

②当采集到 ARP 应答报文时，查找有无相应的请求报文。若无，标记该日志记录，报警提示；若有相应请求报文，再提取其源 IP 地址和源 MAC 地址，查找地址关系库。若有该地址对应关系，将该报文信息存储到日志文件，分析下一条报文；若无该地址对应关系，标记该日志记录，报警提示。

4.2 主要数据结构

以下定义以太数据帧首部结构，用于解析以太网数据帧首部，并收集源 MAC 地址信息，与其对应的源 IP 地址信息，一同存入 IP-MAC 地址映射库。

```
struct ether_header {
u_int8_t ether_dhost[6];/* 目的 MAC 地址 */
u_int8_t ether_shost[6];/* 源 MAC 地址 */
u_int16_t ether_type;};
```

以下结构定义 IP 数据报首部结构，用于解析 IP 数据报首部，并收集源 IP 地址信息，与其对应的源 MAC 地址信息，一同存入 IP-MAC 地址映射库。

```
typedef u_int32_t in_addr_t;
struct in_addr
{ in_addr_t s_addr; };/* 定义 32 位 IP 地址 */
struct ip_header {
    ......
    u_int8_t ip_version:4, /* 版本号 */
    ip_header_length:4; /* IP 首部长度 */
    u_int8_t ip_tos; /* 服务类型 */
    ......
    struct in_addr ip_source_address;/* 源 IP 地址 */
    struct in_addr ip_destination_address;/* 目的 IP 地址 */
};
```

以下定义 ARP 数据报结构，通过分析捕获到的 ARP 应答或请求报文，比较源 MAC 地址、源 IP 地址是否与标准 IP-MAC 地址映射库中的对应关系一致，从而判断该 ARP 报文是否合法。所有的 ARP 报文信息都将存储到日志文件，包括以太帧中的源 MAC 地址、目的 MAC 地址、ARP 数据报中的

源 MAC 地址、源 IP 地址、记录时间等，以供查看分析使用。

```
struct arp_header {
u_int16_t arp_hardware_type;/* 硬件类型 */
……
u_int8_t arp_source_ethernet_address[6];
/* 源 MAC 地址 */
u_int8_t arp_source_ip_address[4];
/* 源 IP 地址 */ u_int8_t arp_dest_ethernet_address[6];
/* 目的 MAC 地址 */
u_int8_t arp_destination_ip_address[4]; /* 目的 IP 地址 */ };
```

检测过程的结果如图 2 所示。

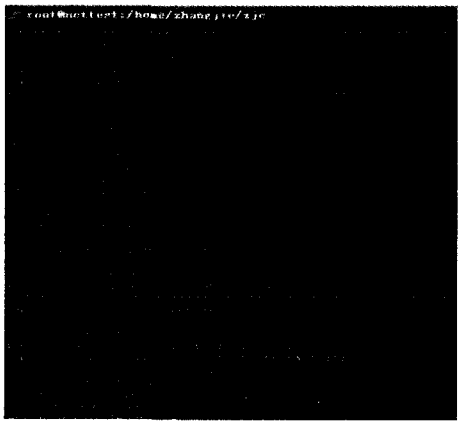

图 2　ARP 欺骗检测分析截图

4.3　检测分析

该检测系统在运行过程中，能够捕获到所有的 ARP 报文，没有发生丢包现象。本文采用 Libdnet 开发库构造 ARP 欺骗应答报文，对系统进行测试。系统能有效检测出欺骗报文，并锁定发欺骗攻击的 MAC 地址。由于 IP-MAC 地址标准对应库是检测出欺骗报文的基础，建立正确完善的地址对应关系至关重要。当采用动态学习的方法建立地址库时，由于系统没有对 IP 地址的范围进行限制，导致地址库中存在大量无用地址对应关系，对地址查找效率产生一定影响。相对地，手工建立地址库的方法保障了其精简和完整性，提高了检测效率。

结束语　ARP 协议在基于 TCP/IP 的网络中广泛应用，虽然因协议固有的安全漏洞，ARP 欺骗会导致网络运行和网络用户受到严重的安全威胁，但通过剖析掌握其攻击原理后，我们可以采用有效的防范措施，来对网络施行保护，减小其危害。本文提出的 ARP 欺骗检测方法简洁易行，可以结合其它防范措施，对检测网段提供安全保障，具有一定的实用价值。

参 考 文 献

1　Stevens W R. TCP/IP Illustrated Volume 1: The Protocols [M]. 北京：机械工业出版社，2000
2　刘凯，邓兰，黄明和. 在局域网中防止 ARP 欺骗的一种方法及其实现[J]. 江西师范大学学报，2005，29(2)：173～175
3　王奇. 以太网中 ARP 欺骗原理与解决办法[J]. 网络安全技术与应用，2007
4　陈辉，陶洋. 基于 WinPcap 实现对 ARP 欺骗的检测和恢复[J]. 计算机应用，2004，24(10)：67～68
5　郑文兵，李成忠. ARP 欺骗原理及一种防范算法[J]. 江南大学学报，2003，2(6)：574～577
6　吕骥，文静华. 校园网内 ARP 欺骗攻击及防范[J]. 福建电脑，2007(5)
7　庄健平. 基于 ARP 协议入侵的安全策略[J]. 怀化学院学报，2006，25(8)：81～83

(上接第 41 页)

单，暂且将与接口 1 相连的网段称为网段 1，其它两个称为网段 2 和 3。汇聚点在网段 1 中，文件源在网段 2 中。

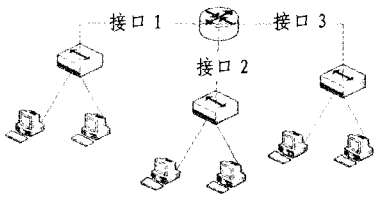

图 6　测试拓扑图

4.2　测试结果

4.2.1　同一网段内

(1)Source Peer

①JXTA 的基本配置

首先配置 Basic 选项卡，填入 Peer Name，Password 等信息；Advanced 选项卡采用默认设置；Rendezvous/Relays 选项卡也选择默认设置。

②运行结果

首先，发现并加入 NetPeerGroup 组，然后在缓存中查找 MulticastGroup。已存在，则加入之，显示出 MulticastGroup 的相关信息，同时显示加入组成功的信息，然后在缓存中查找 InputPipe 信息；若不存在，则创建。若存在，则显示其信息，并且显示成功创建 InputPipe 信息，同时等待其它 Peer 的 Request；收到其它 Peer 的 Request；向请求 Peer 发送 Response；继续等待其它 Peer 的请求。

(2)Reciver Peer

①JXTA 的基本配置

Basic 选项卡：与 Source Peer 相同；Advanced 选项卡：将 Http 的端口号改为手工配置，8000；Rendezvous/Relays 选项卡：采用默认值。

②运行结果

首先，发现并加入 NetPeerGroup 组；接着，发现并加入 MulticastGroup 组；查找管道信息；创建自己的 InputPipe；连接到文件源并向其发送请求；等待文件源的回应，显示 Response 内容，并将其写入配置文件。

4.2.2　不同网段间

JXTA 的配置与同一网段的基本一致，只需在 Rendezvous/Relays 中的 Rendezvous send peers 中添加已设置好的汇聚 Peer 的地址就可实现信息转发。

4.3　结果分析

通过对实验数据的分析，发现仍存在一些问题：①在同一网段的情况，一般很容易实现，同时开启多个 Peer 的时候也可以顺利进行。但是文件源的 Peer 要较其它 Peer 早开启，若晚开启或者同时开启都会出现找不到组的情况。②不同网段间的情况，需设置汇聚点方可通讯。③跨多个路由的情况：由于网络的复杂性，因此会影响到速度，但可以实现文件源的发现，只是速度上较同一网段上的稍慢了一些。

今后将在此基础上对系统的性能、安全性、对多媒体信息的传输等方面进行深入研究。

参 考 文 献

1　丘子隽. IP 组播的概念与应用. 世界宽带网络，2005. 25～30
2　JXTA Java Standard. Edition2. 3. 4Javadoo [EB/OL]. http://platform. jxta. 0rg/n0nav/java/api/jndex. html，2005
3　张智，李瑞轩. 基于 JXTA P2P 的 Web 服务发现模型研究[J]. 计算机工程与应用，2005，41(19)：137～139
4　Gong L. JXTA: A Network Programming Environment[J]. IEEE Internet Computing，2001，15(3)：88～95