文章编号:1674 - 2869(2011)04 - 0103 - 03

简单网络管理协议的 ARP 欺骗防御机制

赵 罡
(孝感学院计算机与信息科学学院,湖北 孝感 432000)

摘　要:通过简单网络管理协议(SNMP)提取网络设备运行状态的相关信息,发现并定位 ARP 欺骗者,然后采取相应隔离 ARP 欺骗者的措施,排除 ARP 欺骗对网络正常运行的危害.

关键词:简单网络管理协议;ARP 欺骗;MIB;主动防御;网络安全
中图分类号:TP393.08　　**文献标识码**:A　　**doi**:10.3969/j.issn.1674-2869.2011.04.027

0 引　言

近年来,有一类叫做 ARP 的病毒开始不断地向各个行业的网络环境扩散,其目的从最初的窃取 QQ、网游、网银等账号,发展到后来专门抢占网络带宽以及纯粹破坏网络通讯等等.2007 年,ARP 欺骗对教育行业的影响达到顶峰.多所国内知名大学网络中心相继发布了专门针对防治 ARP 病毒的公告.这两年 ARP 病毒肆虐大学校园网,严重地干扰着用户的正常上网.

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,它是建立在各主机相互信任的基础上,因此存在一些问题[1].

a. 主机 ARP 列表是基于高速缓存动态更新的.

b. ARP 请求时以广播方式进行.

c. 可任意发送 ARP 应答分组.

d. ARP 应答无须认证.

1 ARP 欺骗原理

针对 ARP 协议的上述漏洞,可以通过定时发送 ARP 应答分组,不断更新被欺骗主机的缓存,就可以达到 ARP 欺骗的目的[2].

为了降低网络数据流量,ARP 处理机制规定当一台主机接收到 ARP 应答后不进行验证就将收到的 MAC 地址映射信息放入 ARP 缓存中,即使该主机从未发出任何 ARP 请求.因此不管真实与否,当某台主机接收到任何 ARP 应答将会更新其地址映射表[3].

利用此缺陷就能进行 ARP 欺骗了.例如:某个局域网内有 A、B、C 等 3 台主机.A 和 B 之间能进行通信,C 在正常情况下无法获得它们的通信数据.但是 C 希望插入到 A 和 B 之间,使 A 和 B 之间的通信都经过 C 转发.这样 C 就可以得到它们之间的通信内容了,容易得到其中的机密.C 的欺骗行为是这样进行的:

A 的 IP 为:192.168.0.1,MAC 为:0A0A0A0A0A0A;

B 的 IP 为:192.168.0.2,MAC 为:0B0B0B0B0B0B;

C 的 IP 为:192.168.0.3,MAC 为:0C0C0C0C0C0C;

A 和 B 各自维护自己的 ARP 表,图 1 是正确的 ARP 表.

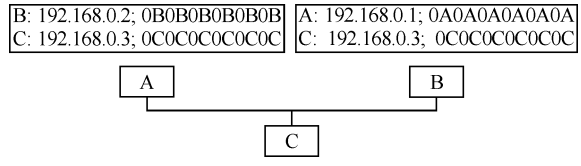

图 1　各个主机各自维护自己的 ARP 表

Fig. 1　ARP table of different main computers

主机 C 开始发送 ARP 的应答信息给主机 A,C 发的 ARP 应答数据包信息为:"IP:192.168.0.2,MAC:0C0C0C0C0C0C",这个信息中,MAC 地址却是主机 C 的,但 IP 地址是 B 的.主机 A 接收到这条 ARP 应答信息后直接修改了自己的映射表,把 IP:192.168.0.2 对应到 MAC:0C0C0C0C0C0C.主机 C 再向 B 发送 ARP 应答包:"IP:192.168.0.1,MAC:0C0C0C0C0C0C",同样的,B 接收到后也修改了自己的地址映射表(见图 2).

2 防御 ARP 欺骗的原理

2.1 防范原理

简单网络管理协议(SNMP)是为基于 TCP/

收稿日期:2010 - 11 - 30

作者简介:赵　罡(1982 -),男,湖北武汉人,助教.研究方向:信息安全.

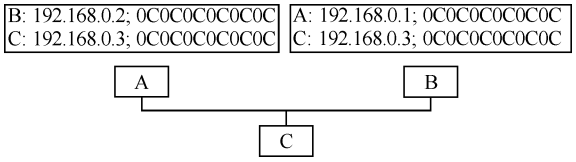

图 2 主机 C 对主机 A 和 B 进行 ARP 欺骗后,主机 A、B 的 ARP 地址表

Fig. 2 ARPtable of main computer A and B after ARP deception by main computer C

IP 的多厂商异构互联网的管理而设计. 它作为工业标准,已被广泛接受,其应用已扩展到其它协议组. 目前几乎所有的网络产品,包括交换机、路由器、UPS、MODEM 等硬件以及许多软件均支持 SNMP. SNMP 的基础是 MIB 数据库,MIB 数据库包含了所有被管对象的信息. 网络中的所有系统(包括工作站、服务器、路由器、网桥等)都有反映系统中被管对象状态的 MIB. 网络管理实体可提取 MIB 中的对象值监来测系统中的资源,也可以通过修改这些对象值来控制资源. MIB 变量将记录各个相连网络的状态、通信量数据、发生差错的次数以及内部数据结构等当前内容. 与 ARP 欺骗相关的信息就可以通过这些 MIB 变量获取,并且通过 MIB 库定义的其它 MIB 变量可以设置网络设备的运行参数,从而将实施 ARP 欺骗的终端隔离开来,阻止 ARP 欺骗对网络正常通信的破坏[4].

SNMP 的管理信息库采用树型结构,它的根在最上面,根没有名字. 每个 MIB 对象都用对象标识符(OID)来唯一的标识,其中各个可用信息是带标号的节点,每个节点用数字和字符显示,其中对象标识符 OID 是由句点隔开的一组整数显示,也就是从根节点通向它的路径,其命名节点并指示它在树中的准确位置. 图 3 是管理信息库的一部分,又称对象命名树(object naming tree). 从图 3 中可看出,在讨论 Internet 的对象时,只要给出 Internet 以下的子树(图中的波浪线方框),并在其结点旁标注{1. 3. 6. 1}即可. 在 Internet 结点下的第二个结点是 mgmt,标号为 2. 再往下是管理信息库,其标识为{1. 3. 6. 1. 2. 1}或{Internet(1). 2. 1}. 这种标识称为对象标识符[5].

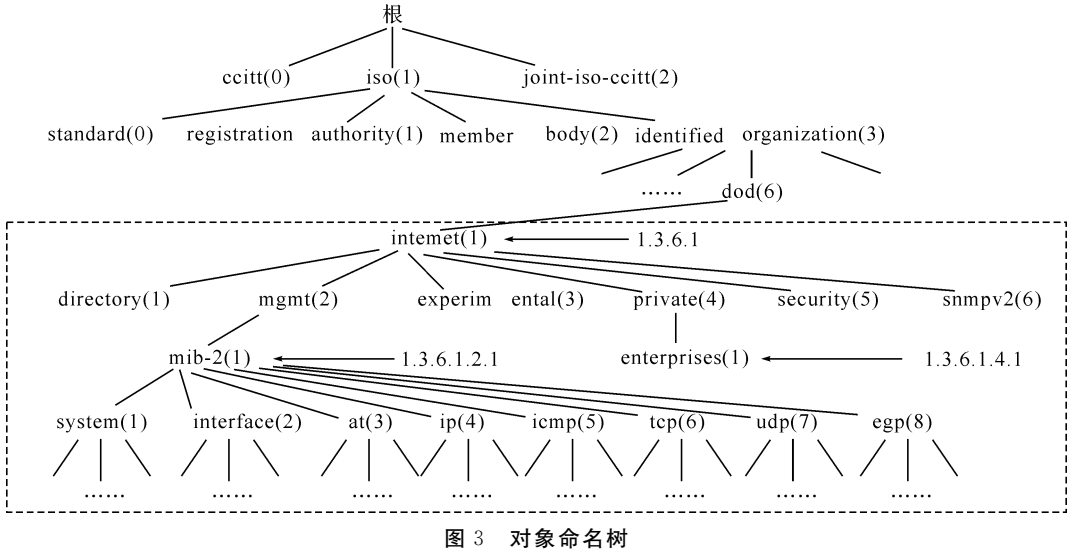

图 3 对象命名树

Fig. 3 Object naming tree

至此,可将此过程的实现分为 3 个步骤:首先检查网络中是否存在 ARP 攻击,并确定 ARP 欺骗者的 MAC 地址;然后找到欺骗者接入交换机的端口;最后将此端口关闭.

2.2 判定是否发生 ARP 欺骗

读取网络里所有 ARP 表,获得对应的 MAC_IP 内容.

该步骤使用 3 个 OID 来得到 ARP 表条目:

OID[0] = "1. 3. 6. 1. 2. 1. 4. 22. 1. 1",得到端口索引号.

然后和 OID[1] = "1. 3. 6. 1. 2. 1. 4. 22. 1. 2" 比较,得到 IP 和 MAC 地址

OID[2] = "1. 3. 6. 1. 2. 1. 4. 22. 1. 4",得到条目类型(静态或动态)

通过遍历 ARP 表中的端口索引值,将获得的 MAC_IP 内容填充表 ALL_MAC_IP 中,然后对此表中的 MAC 和 IP 进行判断,若出现了一个 MAC 对应多个 IP 的情况,则说明出现了 ARP 欺骗.

2.3 定位 ARP 欺骗源

定位欺骗源,主要思想是利用 MIB 库中的 FDB 表,也就是 MAC 地址转发表:首先用 FDB 表找到欺骗源在交换机上的转发端口,然后再看这个端口是否还和别的交换机相连,如果还有相连的交换机,那么查找过程就会从这个端口转到此

交换机上;如果此端口没有和别的交换机相连,那么这个端口就是欺骗源所在的端口,定位完成[6].

这个过程可分为以下 4 步:

1)根据此 MAC 地址,找到其对应于链路层 FDB 表中的 MAC 地址,然后通过此地址找到 FDB 表中的端口.

2)根据上步找到的端口,到 FDB 表中找到其对应的端口索引值.

3)用上一步找到的端口索引值和每个设备对象的相邻设备表进行比对,就能找到其相应的端口或者交换机 IP. 相邻设备表需要预先在网络管理系统中对每个设备对象添加,表中的内容包括对象和接口.

4)在第 3)步的比对中如果找到的是交换机 IP,说明发往该目的 IP 设备的数据包是通过相邻交换设备转发的,那么下一步查找就在相邻交换机上进行. 也就是从步骤 1)开始新的查找. 如果第 3)步没有得到交换机的 IP,那么找到的端口就是所需端口,查找也就可以结束了[7].

在定位端口的过程中涉及的 MIB 变量如下:

FDB 表中的 MAC 地址(dotldTpFdbAddress):1.3.6.1.2.17.4.3.1.1

FDB 表中的端口索引值(dotldTpFdbPort):1.3.6.1.2.17.4.3.1.2

2.4　隔离 ARP 欺骗源

由以上的几步操作就得到了欺骗源对应的交换机端口,那么关闭这个端口就能阻止欺骗的发生了.

交换机的每一个端口都有与之对应的 MAC 地址,在每一台交换机中均维护着这样一个 MAC 地址表,表中还记录了任何与交换机相连的主机的 MAC 地址. 端口的关闭可以通过改变实时的 Switch－Port－MAC 对应表的管理状态来实现. 此表可以通过 SNMP 管理站与各个交换机的 SNMP 代理通信保存的与端口对应的 MAC 地址表而获得.

在 MIB 表中有一个可读写对象 ifAdminStatus(对象标识符号为 1.3.6.1.2.1.2.2.1.7),此对象代表端口管理状态. 给其赋不同的值,可以改变端口的状态:“1”——开启端口,“2”——关闭端口,“3” ——测试. 给交换机发送赋值信息(Set Request),就可以关闭和开启相应的端口. 比如要关闭的是交换机 192.168.42.157 的 22 号端口,可以向该交换机发出如下信息:

set(“private” 192.168.42.157 1.3.6.1.2.1.2.2.1.7.22.0.2).

3　结　语

本文介绍了利用简单网络管理协议实现 ARP 欺骗的防御过程,实现了在普通 PC 机上查询 ARP 表以及查询任何一台终端所对应的交换机端口. 针对 ARP 攻击提出一种新的防御模式,该模式通过查找欺骗源,并将其接入网络的端口主动断开达到对 ARP 攻击的主动防御. 该方案主动发现与处理 ARP 欺骗问题,特别适合在较大规模的网络中部署,代价小,效率高.

基于本文所提出的防御模式设计了一套主动防御的方案,这套方案在学校机房监控了 20 多台网络设备及 300 多个网络终端,实践证明该方案能及时发现并处理其中任何一个或多个终端的 ARP 欺骗行为.

参考文献:

[1] Tanenbaum A S. ComputerNetworks(Third Edition)[M]. 熊桂喜,王小虎,译. 北京:清华大学出版社,2001.

[2] 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(2):42－44.

[3] 王佳,李志蜀. 基于 ARP 协议的攻击管理分析[J]. 微电子学与计算机,2004(4):10－12.

[4] 秦耀东. 网络流量采集与分析系统中 SNMP 代理的研究与实现[D]. 广州:华南理工大学,2004.

[5] 黄勇. SNMP 网络管理系统的设计与实现[D]. 成都:电子科技大学,2003.

[6] 李佳,石冰心. 基于 ICMP 和 SNMP 的网络拓扑发现算法研究及实现[J]. 微型机与应用,1998(1):32－34.

[7] 肖科,许晓东,肖叶. 基于 SNMP 的用户 IP 定位方案的研究[J]. 微计算机信息,2007(33):100－102.

(下转第 110 页)