基于多元绑定的校园网 IP 盗用解决方案探讨

A Solution to the Embezzlement of Campus Net IP Address Based on Multi – colligation

褚建立　（邢台职业技术学院 河北邢台 054035）

摘要：随着校园网应用的深入和终端用户的增加，使得 IP 地址盗用十分普遍。严重影响网络管理，给网络管理人员和网络用户带来很大麻烦。本文从 IP 地址盗用的常用手段入手，分析了目前常用的防止 IP 地址盗用的防范技术，提出了一种基于 802.1x 的多元绑定的校园网 IP 防盗系统。

关键词：多元绑定　校园网　Radius　802.1x

1　引言

随着校园网应用的深入和终端用户的增加，在用户管理和安全管理上的问题凸现出来，其中 IP 地址冲突现象特别明显，使合法用户不能使用网络资源，造成网络工作不正常。解决 IP 地址冲突、实现用户的唯一性确定，成为维护网络健康、安全运行的重要任务。

2　IP 地址盗用的常用手段

IP 地址的盗用方法有多种多样，其常用方法主要有以下几种：

2.1　单纯修改静态 IP 地址

如果用户在配置 TCP/IP 或改动此配置时，使用的是未经合法分配的 IP 地址，就形成了 IP 地址的静态盗用，而网络管理员无法限制用户对地址的静态修改。

2.2　成对修改 IP – MAC 地址

在一些采用兼容网卡的计算机上，如果将一台计算机的 IP 地址和 MAC 地址都改为另外一台合法主机的 IP 地址和 MAC 地址，这就形成 IP – MAC 地址成对盗用，这时控制修改静态 IP 地址的防盗用措施（如静态路由技术）就无能为力了。

2.3　IP 电子欺骗

所谓 IP 电子欺骗，就是伪造某台主机的 IP 地址的技术。IP 欺骗通常需要用编程来实现。通过使用 SOCKET 编程，发送带有假冒的源 IP 地址的 IP 数据包。对于网络黑客高手来说，绕过上层网络软件，动态修改自己的 IP 地址，达到 IP 欺骗并不是一件很困难的事。

3　常见 IP 地址防盗方案

针对 IP 地址盗用问题，网络管理员采用了各种防范技术，现在比较通常的防范技术主要是根据 TCP/IP 的层次结构，在不同的层次及不同的网络环境中采用不同的方法来防止 IP 地址的盗用。

3.1　通过交换机端口进行控制

交换机工作在 TCP/IP 第二层，利用交换机端口进行控制可以起到一定的作用，在交换机的端口上可以设置端口与 MAC 的绑定关系、端口与 IP 的绑定关系以及将端口配置为单地址工作模式。

3.2　路由器隔离

采用路由器隔离的办法是通过 SNMP 协议定期扫描校园网各路由器的 ARP 表，获得当前 IP 和 MAC 的对照关系，和事先合法的 IP 和 MAC 地址比较，如不一致，则为非法访问。

路由器隔离技术能够解决 IP 地址的盗用问题，但是如果非法用户动态的修改 IP 地址或成对修改 IP – MAC 地址，对这样的 IP 地址盗用它就无能为力了。另一方面，当 IP – MAC 表较大时会严重影响路由器的性能。

3.3　防火墙与代理服务器

利用防火墙与代理服务器相结合的方案建立 IP – MAC – USER 三元模型，通过身份认证取得访问网络的权限才能够访问外部网络。使用这样的办法是将 IP 防盗放到应用层来解决，将 IP 地址的管理转换成对用

户及口令的管理。此方法可以很好解决盗用者访问外部网,对于同时盗用 IP 地址和 MAC 地址的盗用行为有一定的作用。

使用防火墙和代理服务器的缺点也是明显的,对于非法用户盗用内部网合法用户 IP 地址无能为力,并且由于使用代理服务器访问外部网络很容易产生瓶颈问题,在一定程度上会影响用户访问网络的速度。

3.4 利用 DHCP 技术防止利用代理服务器形式的盗用形式

可以利用 TCP/IP 协议栈的 DHCP 协议进行 IP 地址的分配,让用户每次获得不同的 IP 地址,从而让代理行为的盗用失效。在进行 DHCP 的配置时要启用配置交换机的 DHCP Snooping 和 Dynamic ARP Inspection 功能防止 IP 地址的盗用。

3.5 基于 ARP 伪装技术的防盗模型

哈尔滨工业大学的研究人员提出了一种基于 ARP 伪装技术的防盗模型。基于 ARP 伪装技术的 IP 防盗用系统采用纯软件的解决办法,具体方案为在每个子网内安装一个 IP 防盗用软件系统,并建立子网内合法用户的 IP 地址 – MAC 地址 – IP 开关状态标志(记录有合法用户的 IP 地址和 MAC 地址,IP 开关状态标志由用户自行管理。当用户要退出网络时,访问 IP – MAC 地址库,将分配给他的 IP 地址所对应的开关状态标志项设置为关闭;当用户重新使用网络时,再次访问 IP – MAC 地址库将开关状态标志打开)由 IP 防盗用软件根据子网的 IP – MAC 地址库实现 IP 地址与主机 MAC 地址的绑定,任一子网内的主机只有使用在 IP – MAC 地址库中登记的且与其 MAC 地址对应的 IP 地址,才能进行正常的网络通信,从而在整个校园网实现 IP 防盗用。

该方案对成对修改 IP – MAC 地址和动态修改 IP 地址的 IP 地址盗用方式进行一定的防范,但此方案的缺陷是每个子网都要安装 IP 防盗用软件系统,给网络管理员的维护工作带来了不便。

3.6 基于透明网关过滤器的 IP 防盗方案

清华大学计算机与信息管理中心提出了一种基于透明网关过滤器的 IP 防盗方案。即结合静态路由和防火墙的优点,使用 IP – MAC – USER 三元模型来进行授权验证,以实现防止 IP 地址盗用。其工作原理是:实现一个透明网关 Fitler,该网关跨接在内部网络和外部网络之间,对于内部主机访问外部网络,在使用 ARP 获取外部主机或路由器地址时,验证其 IP – MAC 地址对,不匹配的非法主机不能获得 ARP 应答信息,因而不能继续和外部网络通讯;对于外部主机访问内部网络,则采用静态路由,使 IP – MAC 地址对不匹配的内部主机接收不到正确的 IP 包。另外,为了防止 IP – MAC 地址成对修改的情况,在外部 IP 包经过透明网关时,如果其源地址为国外主机,则还要检测其目的主机是否有用户注册,若没有用户注册,则其 IP 包被丢弃;有用户注册则 IP 包被转发进去,同时将 IP 流量记入该用户的帐上。这样,即使用户成对修改了 IP – MAC 地址,如果没有合法的用户注册,它仍不能访问外部网络,盗用 IP 地址失去意义。

此方案能够有效发现 IP 盗用事件,但是不能实现定位和反向追踪盗用行为,即无法获知盗用者。

3.7 利用 MAC 地址动态配置防止 IP 地址盗用方案

中南大学信息科学与工程学院黄家林高级工程师提出了一种利用 MAC 地址的动态配置防止 IP 地址盗用的方法。本方案的工作原理是:设计一个客户端软件。该软件事先需要所有合法用户申请并获得一个用户名和密码。该客户端利用加密技术与系统通信。系统在通过身份认证后,客户端在用户关机前,向系统申请修改其 MAC 地址。系统收到申请后,在整个内部网络范围(以边界路由器为界)随机动态配置一个 MAC 地址给该主机。该 MAC 地址不与数据库中的 MAC 地址冲突。客户端在收到系统返回的 MAC 地址后,对本机 MAC 地址作出修改,然后正常关机。这样用户在每次开机连入网络时,都使用不同的 MAC 地址,当用户在使用网络时,盗用者即使通过某些手段获取该用户的 IP 地址、MAC 地址对,也无法盗用,因为网络系统会发生地址冲突。当该用户准备关闭计算机时,用户机器向系统申请改变的 MAC 地址,使当前 IP 地址、MAC 地址对应关系失效。这样盗用者将无法盗用 IP 地址、MAC 地址对。

4 基于 802.1x 的多元绑定的 IP 防盗解决方案

从上述论述中可以看出 IP 防盗技术从开始的单纯的绑定技术向综合、高效、低成本、易实施、通用性强的防止 IP 盗用的解决方案方向发展。在这里我们提

出一种采用多元绑定接入控制技术来防止 IP 地址的盗用。如果限制用户只能用自己的帐户、自己的口令、自己的主机(AMC)、采用分配的 IP 地址、采用固定的物理端口接入,如果其中一项不符,认证就不允许通过。这就是多元绑定接入技术的基础。多元绑定接入技术是通过对用户的帐户、口令、IP、MAC、对应的交换机的物理端口、VLAN 等六个元素进行捆绑,以此来实现网络用户接入的有效控制与管理的技术。多元绑定的 IP 防盗示意图如图 1 所示。

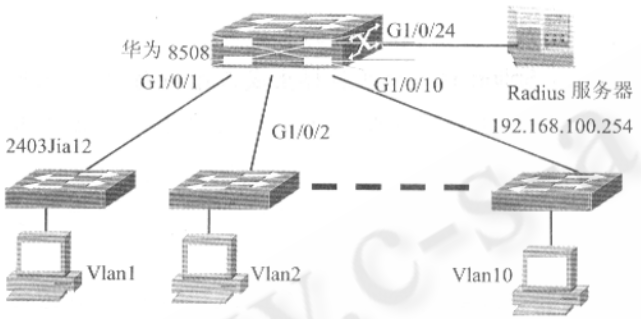

图 1　多元绑定 IP 防盗示意图

4.1 802。1x 认证原理

IEEE 802.1x 协议的体系结构包括 3 个重要的组成部分:客户端、认证系统、认证服务器。

(1) 客户端系统一般指用户终端系统,该终端系统通常需要安装一个客户端软件,用户通过启动这个客户端软件发起 802.1x 协议的认证过程,为了支持基于端口的接入控制,客户端系统需支持 EAPOL[1] (extensible authentication protocol over LAN)协议。

(2) 认证系统通常指那些支持 802.1x 协议的网络设备,一般认证系统运行于 NAS(network access server)之上,给用户提供接入服务。认证系统有两个逻辑端口:受控(controlled port)端口和不受控端口(uncontrolled port)。不受控端口始终处于双向连通状态,主要用来传递 EAPOL 协议帧,用于承载用户的认证信息,可保证客户端始终能够发出或接受认证;受控端口只有在认证通过的状态下才可打开,用于传递网络资源和服务。PAE 是端口访问实体(port access entity),分为客户端 PAE 和认证系统 PAE。客户端 PAE 位于客户端,主要负责响应来自认证系统建立信任关系的请求。认证系统 PAE 位于认证系统,负责与客户端的通信,把从客户端收到的信息传送给认证服务器以完成认证。认证系统的 PAE 通过不受控端口与客户端 PAE 进行通信,两者之间运行 EAPOL 协议;认证系统的 PAE 与认证服务器之间运行 EAP[3] (extensible authentication protocol)协议。

(3) 认证服务器通常为 RADIUS 服务器,该服务器对于认证系统中继的用户客户端信息进行验证,当验证通过时,返回与用户相关的上网信息给认证系统,认证系统根据返回信息进行设置,例如打开受控端口,或者向客户端传送验证失败的信息。

4.2 Radius 服务器

在 Radius 服务器的数据库中都存有每一个接入用户的信息,包括帐户、口令、IP、MAC、对应的交换机的物理端口、VLAN 等。当用户发起认证时,首先要到 Radius 服务器上进行身份认证,Radius 服务器会检验用户认证信息中携带的元素是否与该服务器中与先存有的信息一致,如果一致则认证通过,否则就认为该用户为非法用户而禁止接入;当用户通过了认证后,接入层的交换机与 802.1x 认证客户端之间还会不间断的通过 hello 检测报文进行检测,一旦用户在通过认证后更改自己的 IP 或 MAC,客户端会通知接入层交换机,接入层交换机再上报 Radius 服务器,Radius 服务器将会强制用户下线。

在本文中,使用 FreeRadisu 1.0.2 在 Linux 上构建 Radius 服务器并采用 MySQL 作为后台数据库。

4.3 接入层交换机

用户在 Radius 服务器认证通过后,在接入层交换机上会产生一条 ACL 策略将该用户的 IP、MAC、VLAN、端口进行捆绑,如果此时用户随意更改自己的 IP 地址,交换机将会强制用户下线。用户下线后,对应端口的 ACL 策略会自动释放、删除。在接入层交换机上启用 802.1x 并设置重新认证时间间隔,在用户认证通过后,每隔一个时间间隔,交换机要向用户发起重新认证请求。这样的话,用户在使用网络的过程中,就不能够关闭其 802.1x 客户端软件。

[2403Jia12]dot1x //开启全局 802.1x 特性//

[2403Jia12]dot1x interface ethernet0/1 //开启指定端口 ethernet0/1 的 802.1x 特性//

[2403Jia12] dot1x port - method portbased interface Ethernet 0/1 //设置接入控制的方式(基于端口,默认基于 MAC)//

(下转第 82 页)

(上接第 85 页)

[2403Jia12]radius scheme radius1 //创建 radius 组//

[2403Jia12 – radius – radius1]primary authentication 10.8.100.254 // 设置 Radius 服务器的 IP 地址//

[2403Jia12 – radius – radius1]key authentication password //设置系统与 Radius 服务器交互报文时的加密密码//

[2403Jia12 – radius – radius1]timer 5 //设置重新认证时间间隔//

5 结束语

通过在校园网中采用基于 802.1x 技术的多元绑定技术来防止校园网内部 IP 地址的盗用起到了很好的效果,维护了校园网络的正常运行。

参考文献

1 姚凯、徐建祥, 有线电视宽带网 IP 地址盗用防范技术研究, 中国有线电视, 2005(09/10).

2 翁小兰, 校园网环境下 IP 地址盗用防范技术研究, 微计算机应用, 2005(11).