基于专网的网络访问控制软件研究与设计

楼恒越 窦月皎
(四川师范大学计算机科学学院 成都 610101)

摘 要 在分析专网内部的安全性和保密性以及网络访问控制的需求的基础上,针对对专网内使用有线和无线网卡上网的客户端计算机进行管理和限制的要求,设计并实现了一个基于Windows系统平台的网络访问控制软件。该软件通过检测客户端IP地址改变等消息,触发网络控制事件,实现上网限制和管理等功能,现已经投入实际使用。

关键词 专网,网络访问控制,IP地址改变检测

Research and Design of Network Access Control Software Based on a Special Network

LOU Heng-yue DOU Yue-jiao
(Department of Computer Science, Sichuan Normal University, Chengdu 610101, China)

Abstract Based on analysis of security and confidentiality in a private network and the demand for network access control, a network access control software was designed and realized. Focused on the request of management and limitation for on-line client computers which used chipset/wireless network card in a private network, this software realized its functions by detecting the change of client IP address or other messages, triggering network control events for network monitoring and management.

Keywords Private network, Network access control, IP address change detection

1 引言

专网,即专用网络,也称内网,多用于企事业单位,以解决网络内信息的安全性与保密性问题。在早期的有线网络时代,对于一个区域网络或局域网,在出口处对该网内计算机上网(通常指连接公共网络,或连接外网)的权限进行设定,就可以基本做到专网的对外访问控制。现在,越来越多的计算机开始借助无线网络上网,中国无线上网尽管近几年才起步,但发展却相当迅速。据资料[1]统计,在中国澳门地区的所有网民中,有19%表示有利用手机或手提电脑通过网络供应商提供的无线网络上网,而透过公司/学校/家中架设之WiFi网络上网的网民则有27%,具有无线上网经验的网民达到46%。有报道[2]称"到2013年,全球超过八成宽带用户将以无线方式高速接入互联网"。然而,随着无线网络的覆盖与普及,新问题也随之而来,尤其在一些使用专网的环境中,有线网络可以用传统方法控制上网,而对于无线网络的上网控制则较有难度,主要有以下3类问题:

1)检测难度高。目前流行的使用外置无线上网卡(如3G卡,USB接口无线网卡等),仅在专网出口处检测和控制的传统方法不再有效,对于使用无线网卡上网的计算机,检测其私自连接外网的行为变的比较困难。

2)控制能力低。传统控制网络访问的方法一般是在专网出口处安装防火墙等相关设备,起到对本网内计算机的网络控制,可是当计算机使用无线网卡进行网络连接后,由于防火墙只能控制有线连接,传统方法处理这一问题已捉襟见肘。

3)灵活度低与实时性差。传统的权限管理方式一般是预先设定好网络访问控制权限,而查找违规上网的计算机则需要翻阅日志文件,上网控制的灵活度低、实时性差。

综上所述,针对利用无线网卡进行网络连接的计算机迫切需要一种能够有效检测与控制的工具,以达到保障专网安全性与保密性的要求。

2 网络访问控制软件需求

可信网络是可信计算发展的必然趋势,是下一代互联网发展的必然目标[3],然而,最近,一件网络安全事件却引起了全世界的关注——维基解密网站泄密事件。该网站曝光了大量的美国军事文件以及各种商业机密,其中很多信息的来源正是那些本应属于专网的、存储了重要信息的计算机违规上网而造成的信息泄露。在这个无线网络覆盖率极高的时代,专网中计算机通过无线网络上网所产生的安全威胁是巨大的。所以,对于专网中的计算机,需要专门的工具进行检测与控制,以避免信息泄露与损失。由此,一个全新设计、安全、快捷、有效的网络访问控制软件是人们迫切需要的。

根据调查[4]表明,Windows系列操作系统的市场占有率超过了90%,可见,一个基于Windows平台的网络访问控制软件能发挥极大的作用。以下阐述亦基于Windows平台。

网络访问控制软件需要达到以下几个要求:

1)集中式管理。在一个或几个内网中,一台服务器可以同时管理内网中所有计算机。

2)智能化检测。采用多重检测方式相结合,智能判断计算机违规等级和危险系数。

3)多样化控制。对不同级别的违规现象可以采取不同的处理方式,同一违规现象也可随时调整控制策略。

4)完整的统计。需要记录下所有违规信息并长久保存,具有良好的汇总功能。

3 网络访问控制方式的比较

很多无线网络访问控制的研究是基于Stanford两层结

构[5]。现在防控通过无线网络上网的方式主要有3种：物理阻隔、信息干扰和软件控制。

1)物理阻隔。要做到物理阻隔必须能对AP(无线访问节点)加以掌控，而在实际情况中，用户往往通过周围环境中提供的AP进行网络连接，所以要做到物理阻隔是很难办到的事情。

2)信息干扰。对特定的频率进行干扰会使得利用无线网络上网的用户网络延迟甚至阻塞，但其可以起到一定的作用。然而由于干扰设备昂贵及其使用过程中引起的种种问题，这一方式只在部分特殊环境下才被使用。

3)软件控制。通过安装在用户计算机中的软件对用户上网行为进行监控。控制软件部署方便，效果较为理想，故渐渐成为主流的无线网络防控手段。

4 网络访问控制软件的特点分析

网络访问控制软件是以Windows底层编程为基础，充分利用C/C++语言的高效性，与Windows系列操作系统的全面兼容及其提供的安全性，全面而有效地保障了对计算机网络访问的控制。它的主要特点有：

1)检测及时。通过双重检测手段——动态监视新上网设备的添加与定时探测计算机与外网的连通性，尽可能在最短的时间内检测到违规连接外网的计算机，有效降低了由于检测时间过长而导致的信息泄露的危险性。

2)控制多样。提供了多种选择，如关闭特定端口、禁止连接网关、禁用网卡等多种手段进行不同级别的防护，令有泄露危机的计算机与外界隔绝，达到网络访问的控制和管理，使其能处在一个安全的环境中正常工作。

3)信息反馈。对于那些违反了规定，私自连接外网的专网内计算机，不仅能做出及时的判断，保证信息的安全，同时能上传违规计算机的相关信息至内网服务器，并保存到数据库中，以便及时查阅与统计。

4)状态检测。软件采用“心跳”技术，实时反应当前客户端状态。当客户端软件被手动关闭或阻止运行时，服务器端会及时显示其异常状态，方便管理人员采取相应的措施。

5 网络访问控制软件的设计

本文设计的网络访问控制软件的连接环境如图1所示。客户端与服务器端连接组成一个局域网，处于本网内的计算机在没有得到服务器认证授权前无法直接连接外网。若客户端计算机违规使用无线网卡进行网络连接，则网络访问控制软件会及时上报服务器并作出相应处理。

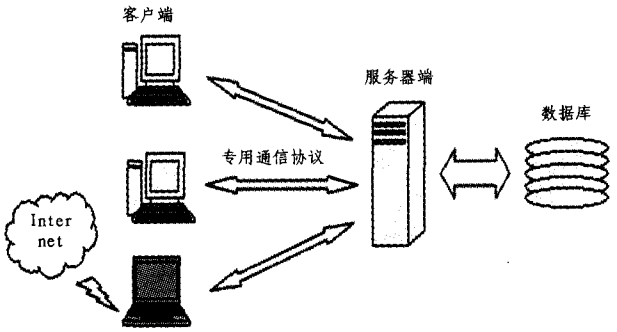

图1 网络访问控制软件的连接环境

软件逻辑流程如图2所示，客户端软件检测到用户计算机有连接外网趋势或已连接外网时，触发网络控制事件，并通过专用通信协议向服务器询问许可。服务器端软件通过与数据库中的信息进行比对，回应是否放行、若需阻止应采取怎样的措施等消息。客户端收到回应后执行相应操作。

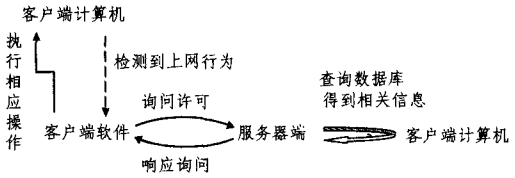

图2 逻辑流程图

网络传输部分有两种协议选择：TCP和UDP协议。TCP协议提供了可靠的面向流的传输方式，与此同时也因其传输前的三次握手规则会消耗部分网络资源；UDP协议是简单的不可靠的传输协议，它并不保证报文的准确送到，但UDP的即发即收机制不会占用很多带宽就能完成传输。因本软件是一个微型软件，并不打算在传输层编写大量程序以达到可靠的传输效果，故采用TCP协议进行传输。利用TCP协议的可靠性与基于字节流的优点来达到传输目的，同时能提高程序编写效率。

网络访问控制软件设计共分为4个部分：客户端设计、服务器端设计、数据库设计以及通信协议设计。

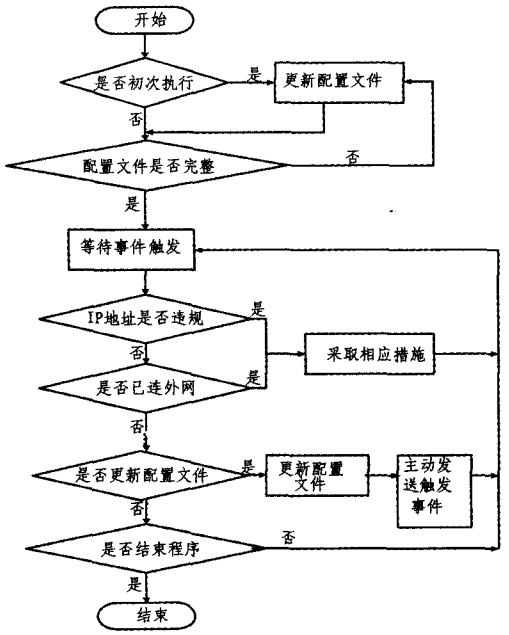

图3 客户端流程图

1)服务器端需要完成的主要功能。对配置文件的设定与修改，对客户端上报的违规信息做出响应并显示在服务器端列表中，同步存入数据库，统计汇总违规信息。服务器端分为4层：界面交互层，提供配置信息浏览、异常信息查看、信息统计等功能；业务逻辑层，提供数据访问层和网络层之间的交互，为界面层提供数据操作接口；数据访问层，提供对数据库数据的操作和网络数据的操作；网络层，处理来自网络的交互，为客户机提供配置文件，为界面提供主机异常信息。

2)客户端需要完成的主要功能。对违规连接外网的客户端计算机进行检测，及时上报服务器端，并做出相应的处理。如图3所示，客户端需要开机启动并对配置文件进行完整性检查以防止被破坏而无法正常使用。随后启动线程分别检测

是否新增上网设备和定时检测是否连接外网，若出现违规情况则做出处理。同时客户端程序是一个后台运行程序，可以使其在不干扰用户正常使用的前提下进行检测与防范。

3)数据库设计经过了优化，满足 BCNF 范式，保证了数据的完整性，同时避免了冗余。

4)设计了专用的通信协议，以减少网络载荷、防止网络拥堵。报文利用密码加密，防范信息被截取利用。网络访问控制软件中，客户端与服务器端主要交互内容有：更新配置文件、上报违规信息及在线状态。使用的信息控制报文格式与交互时序图分别如图 4 和图 5 所示。

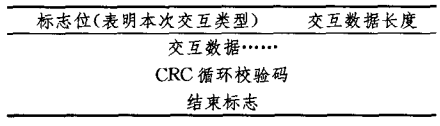

图 4　信息控制报文格式

注：当传递配置文件时，不同条目之间用特定间隔符间隔

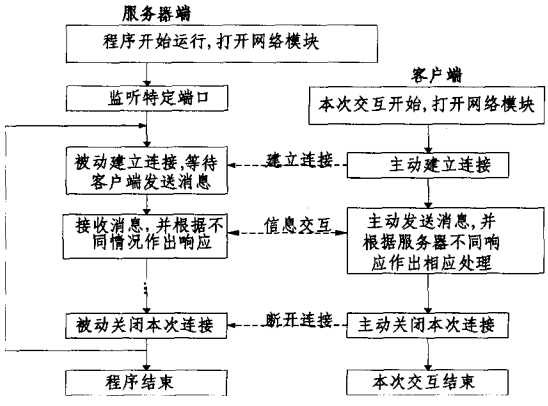

图 5　程序交互时序图

6　网络访问控制软件的实现与测试

本文设计的网络访问控制软件采用通用数据库系统，便于快速查找和访问数据。编码上，客户端使用 C/C++语言编写，执行效率高；服务器端使用了 C# 语言，其稳定的特点，保证了服务器程序可以长期而稳定的运行。软件运行界面如图 6 所示。注：因客户端软件需不影响客户使用计算机，故该软件为后台运行程序，没有界面截图。

在程序的实现中，发现 USB 网卡与一般网卡不同，需要单独处理。因每个 USB 驱动有其唯一的一个 Driver 对象[6]，故本程序采取调用系统函数获取网卡驱动 Driver 对象并做出相应对策限制 USB 网卡的上网行为。

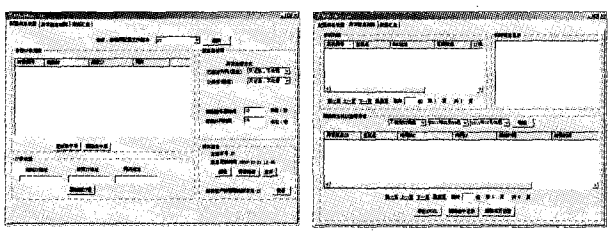

图 6　服务器端程序运行截图

测试之一是用 Windows 自带的 ping 命令不停地探测一外网站点，当服务器端设置为禁止连接外网后，客户端无法 ping 通这一站点；当服务器端重新设置为恢复连接外网后，客户端又能再次 ping 通该站点。客户端计算机使用双网卡，其中有线网卡通过交换机连接服务器，此内网不连接到外网，客户端计算机另有一张无线 3G 网卡，计算机可通过此无线网卡连接外网。

在测试中，当服务器端下达禁止连接外网功能后，客户端几乎在同一时间执行了相应处理，使得计算机无法再通过无线网卡连接到外网。而恢复连接后，在很短的时间内，客户端计算机便可以正常地进行外网连接。测试中，网络访问控制软件快速、有效地达到了需要限制与恢复网络访问的目的。

同时，也针对于软件禁止上网的效率进行了测试。如图 7 所示，在默认设置下(默认设置：检测间隔时间为 5s)，从用户连接上互联网到被软件断开网络连接，平均用时 2.93s。考虑到检测已连接外网所需的延迟，这一测试时间是在可接受的范围内。而在其他测试中，若设置检测间隔时间为 1s，该软件的 CPU 占用率也仅仅为 2%。

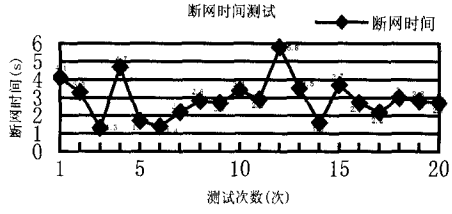

图 7　软件断网时间测试结果图表

由于篇幅所限，在这里着重描述网络访问控制软件的核心代码之一——NotifyAddrChange 函数的调用。

NotifyAddrChange 函数是微软在 Windows 中未公开函数之一，其在 MSDN[7] 上的描述如下：

The NotifyAddrChange function causes a notification to be sent to the caller whenever a change occurs in the table that maps IPv4 addresses to interfaces.

只要当 IPv4 地址列表发生变化时，该函数将发送一个通知告知调用者。当一个新增网络设备需要连接网络时，都需要获取一个 IP 地址，一旦成功获取 IP 地址，网络访问控制软件就会接收到一个由 Windows 发出的通知，告知现在本机 IP 地址发生了改变，这时客户端程序就需要对新获取的 IP 地址加以判断，看其是否在规定范围内，若违规则采取相应措施。主要代码如下：

```
int NotifyIPChange:: NotifyIPChanged()
{
  overlap. hEvent=WSACreateEvent();
  hand=NULL;
  ret=NotifyAddrChange(&hand,&overlap);
  //调用函数 NotifyAddrChange 获得"IP 改变"的事件
  if(ret ! =NO_ERROR)
  {
    if(WSAGetLastError() ! =WSA_IO_PENDING)
        return ERROR;
    }
    if(WaitForSingleObject(overlap. hEvent,INFINITE) ==WAIT
      _OBJECT_0)
    return TRUE;  //IP 地址已发生改变
  return ERROR;
};
```

(下转第 98 页)

资源(R)。网络安全风险分析(Analysis)是网络防御的首要环节,主张通过风险评估与控制机理,预期网络系统的安全风险,为确定安全策略提供依据;安全防御策略(Policy)指导防御技术手段的有效实施,在整个网络安全防御中处于指导地位,是防御体系的核心。技装资源(Resources)包括力量、装备和技术等网络防御资源。网络防御的主要力量源自新型网络对抗装备武装并掌握网络对抗技术的网络士兵。

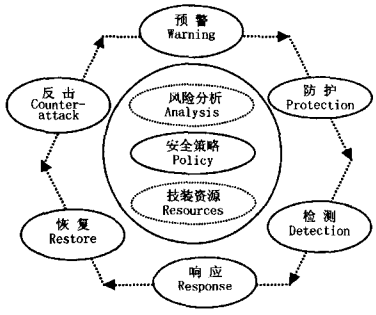

图3 军事网络防御APR-WPDRRC模型

6种技术手段WPRDRRC:W(预警)+ P(防护)+ D(检测)+ R(响应)+ R(恢复)+ C(反击)。它是在PDR中融入纵深防御层级架构技术,并在PDR前增加了预警(Warning),在其后增加了恢复(Restore)和反击(Counterattack),使防御体系具有较强的时序性、可控性和协作性,突出了网络防御要从"事前"(攻击发生前)的入侵预警+安全防护、"事中"(攻击发生时)的动态检测+实时响应、"事后"(攻击发生后)的灾难恢复+精确反击3方面全程考虑,强调了在加强安全防护的同时,还要形成对攻击威胁的快速反应;也强调了在提高网络系统抗击能力的同时,更突出了系统被攻陷后的恢复和反击能力;还强调了闭环控制下反馈机制的形成,更注重了系统防御能力的动态提升。从逻辑层次上,WPDRRC是以WPD实现积极主动防御,以RRC实现系统整固防御,6种技术手段轮式往复,构成了一个具有闭环控制机制的纵深防御模型。其中:入侵预警(W)通过建立有效的"预警反应"机制,当发现网络违规模式和未授权的网络访问尝试时,预警系统能够根据系统安全策略快速反应,如报警、跟踪、封堵和隔离等。目前出现了基于过程推理的预警系统、代理型防火墙预警系统、IDS与FW联动预警系统等;安全防护(P)、动态检测(D)和实时响应(R)中融入线性层级纵深防御的技术手段,在检测到网络入侵攻击之后能包括做好实时响应方案中的一切准备工作,从而把系统调整到安全状态;灾难恢复(R)是由灾难评估、安全恢复、修补漏洞、重构系统等诸多提升网络系统生存能力的技术手段组成;精确反击(C)是通过修复系统、封堵漏洞、追踪并精确定位攻击源,迅速组织力量,采用网络僚机技术、告警与取证技术、攻击源追踪技术、网络攻击诱骗技术等展开快速反击。

在APR-WPDRRC模型中,外围是依次连接的6种技术手段环节构成的同心六边形,内层是依据、策略、资源构成的六边形的核。依据是前提,策略是核心,资源是保证,3者紧密协作,6种技术手段有机联动将预期的安全防御策略变为安全现实。通过组织网络攻防仿真试验,验证了该模型在对抗大规模、分布式、瞬时万变的网络攻击时具有良好的适应性、应变性和耐攻击、强生存的能力,不仅能有力地抵御多种已知的网络攻击,而且也能主动地防御新型的未知的入侵攻击。

结束语 本文提出的纵深防御模型对建立一个全方位的军事网络安全体系具有一定的理论研究和现实意义。从系统整体性出发,进一步的研究需要完善模型整体功能,如融入基于蜜网的网络诱骗防御技术、基于免疫的动态检测技术和基于网格的协同联动防御技术等,建立起平战结合、技术管理一体、综合完善的多层次、多级别、多手段纵深防御的军事网络系统安全体系。

参考文献

[1] 卢昱,等. 协同式网络对抗[M]. 北京:国防工业出版社,2003

[2] 肖军模. 网络信息安全与对抗[M]. 北京:解放军出版社,1999

[3] 陈亚东. 网络攻击与防御[M]. 北京:国防大学出版社,2007

[4] 刘升俭. 网络对抗技术[M]. 长沙:国防科技大学出版社,2008

[5] 樊莉. 军事信息系统安全防御体系建设探讨[J]. 计算机安全,2009(2)

(上接第91页)

其流程如图8所示。

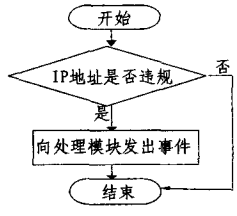

图8 NotifyAddrChange函数的调用及其相关流程

结束语 本文就特殊专网中的网络访问控制进行了探讨,设计并实现了一个网络访问控制软件。所设计的软件经过测试,其稳定性保证7*24小时工作,达到了既定的网络控制管理的功能,并在实际运用中达到一定的效果。但该软件任存在不足,如网络传输部分可以改为带宽占用更少的UDP协议进行传输,在对IPv6的兼容方面仍需改进以适应将来的网络环境,以及服务器端的界面设计可以更人性化等。

参考文献

[1] 中国互联网络信息中心(CNNIC). 第27次中国互联网络发展状况统计报告[R]. 2011

[2] 网易. 科技板块[OL]. http://tech.163.com/09/1120/07/5OH-VMPTU000915BE.html

[3] 封富君,李俊山. 新型网络环境下的访问控制技术,2007.04:17

[4] 中国业界资讯站[OL]. http://www.cnbeta.com/articles/129265.htm

[5] Faria D B, Cheriton D R. DoS and authentication in wireless public access networks[C]//Proc. of the 3rd ACM Workshop on Wireless Security. New York:ACM Press,2002:47-56

[6] 汪涛. 无线网卡驱动程序设计与实现技术研究[D]. 西安:西北工业大学,2005

[7] MSDN(Microsoft Developer Network)[OL]. http://msdn.microsoft.com/