局域网网线软件锁的设计与实现①

翁健高, 易向阳

(广西大学 计算机与电子信息学院, 南宁 530004)

摘 要: 系统基于 TCP/IP 中的 ICMP 协议的工作原理, 利用 VB6.0 编程语言封装 ICMP 数据包, 并通过 Windows 操作系统 API 网络接口函数在局域网中发送, 从软件开发的角度探索网线软件锁的实现方法和步骤.

关键词: ICMP 数据包; Windows 操作系统 API 函数; 网线软件锁

Design and Application of Network Cable Soft Lock

WENG Jian-Gao, YI Xiang-Yang

(School of Conputer, Electonic and Information, Guanxi University, Nanning 540003, China)

Abstract: The system is based on the working principle of TCP/IP ICMP protocol. First it uses VB6.0 programming language to encapsulate the ICMP data packets. Then, it sends ICMP data packets through API network interface function of Windows operating system in the LAN. This article explores implementation methods and steps of network cable software lock from software development perspective.

Key words: ICMP data packets; Windows operating system API; network cable soft lock

目前, 大部分高校计算机实验室全部配置为多媒体网络教室, 每一个多媒体网络教室都安装了南软或远智多媒体教学软件. 在上课过程中, 只要多媒体教学软件的教师端在屏幕广播状态, 则教室中所有启动的学生机都应该被教师机控制并进行屏幕广播接收状态, 这是一款比较先进的屏幕教学软件, 对于计算机的交互式教学很有帮助, 教学效果也很明显, 但是该软件有一个致命的弱点: 只要学生拔除网线或在教师广播教学之前禁用网卡或改动IP地址, 该台计算机就脱离了教师机的控制, 学生摆脱教师机控制的目的基本上是在课堂上看视频电影或玩单机游戏. 在一个公共的教学场所, 在上课期间即使有很少部分学生不自觉地玩游戏, 对课堂也造成很不好的影响, 使得在其周围的同学都不能安心学习. 为了杜绝这种现象的再发生, 特展开 “局域网网线锁”项目的研究. 本项目利用软件设计的方法实现, 软件所协及的知识有 Windows 操作系统 API 函数、TCP/IP 和 ICMP 协议等方面的内容, 所用的编程语言为 VB6.0.

1 软件的工作原理

软件是基于 TCP/IP 中的 ICMP 协议工作的. ICMP 是(Internet Control Message Protocol)Internet 控制报文协议. 它是 TCP/IP 协议族的一个子协议, 用于在 IP 主机、路由器之间传递控制消息. 控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息. 这些控制消息虽然并不传输用户数据, 但是对于用户数据的传递起着重要的作用.

ICMP 协议用于传输出错报告控制信息, 是 TCP/IP 协议族的一个子协议,属于网络层协议,主要用于在主机与路由器之间传递控制信息,包括报告错误、交换受限控制和状态信息等. 当遇到 IP 数据无法访问目标、IP 路由器无法按当前的传输速率转发数据包等情况时, 会自动发送 ICMP 消息.

ICMP 提供一致易懂的出错报告信息. 发送的出错报文返回到发送原数据的设备, 因为只有发送设备才是出错报文的逻辑接受者. 发送设备随后可根据 ICMP 报文确定发生错误的类型, 并确定如何才能更好地重发失败的数据报.

根据 ICMP 协议工作原理, 要想实现网线软件锁的功能, 只要抓取由管理员初始设置的本机的 IP 地址, 然后利用此 IP 地址构建 ICMP 网络数据包, 调

① 收稿时间:2012-05-16;收到修改稿时间:2012-07-03

用 Windows 操作系统的网络接口发送 ICMP 数据包，根据发送数据包后返回的应答状态判断网路是否连通来检测网线是否被拔除或网卡被禁用或本机 IP 地址被改动. 如果检测到网路有故障，则弹出网路故障提示框，并在 15 秒钟后注销计算机，从而使该台计算机只有在插上网线后或解除网卡禁用或将 IP 修改回原地址后才能正常使用.

由于计算机的 IP 地址在 Windows 操作系统中的设置是开放的，可以根据 IP 地址的构成规则任意设置，但在同一局域网中，只有设置同网段的 IP 地址，局域网中的计算机才能相互连通，如果有一用户将本机 IP 修改为不同网段的 IP 地址，则该台计算机独立于整个局域网之外而不受教师机屏幕广播控制. 为了杜绝用户通过修改本机 IP 来摆脱屏幕广播的控制，软件在首次运行时必须先抓取管理员初始设置的本机的 IP 地址，并记录入操作系统的注册表中，以后每次开机，软件自动启动并读取记在注册表中的 IP 为目的地址构建 ICMP 数据包进行发送，才能实现网路的监控；另外，软件是在操作系统的后台运行，运行过程中没有操作界面. 在软件的使用过程中，由于不可预测的原因，致使交换机损坏造成网络物理故障，该故障会引起的软件假报警而使计算机工作异常，在软件内部还应设置操作热键，方便管理员呼出管理界面，输入密码后解除软件的网络监测功能.

2　软件的工作流程

软件采用模块化的设计模式，软件流程图为.

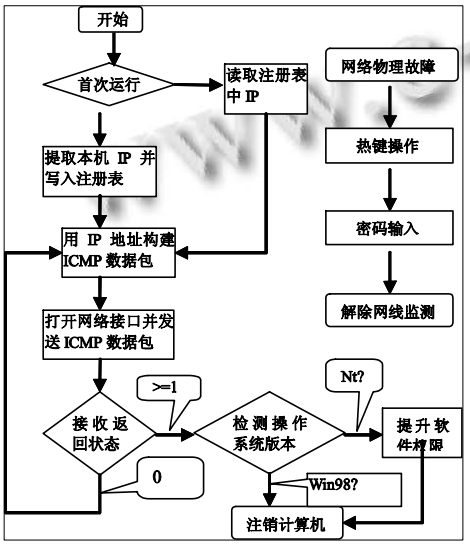

图 1

3　软件实现

(1)实现软件的自动启动功能:

在 Windows 操作系统中，让软件实现开机自启动的方法通常有三种: 一是软件安装完后将软件的应用程序拷贝到 c:\documents and setting\all users\[开始]菜单\程序\启动的系统文件夹中；二是在注册表的根键分支 :HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 路径中添加启动信息；三是把软件注册为系统服务. 第一种方法操作简单，但对于计算机数量较多的局域网机房，工作量会很大，操作显得麻烦和笨拙，不利于软件的推广应用；第三种方法软件编写复杂，增加了软件的设计难度. 本软件随机启动的方式选用在注册表中注册开机自启动的方式进行.

(2)构建 ICMP 数据包并发送，这是软件的核心步骤

①先利用 AddressStringToLong 函数将十进制的 IP 地址转化为 16 进制的数据，实现方法为:

```
Function AddressStringToLong(ByVal temp As String) As Long
Dim I As Integer
Dim pts(1 To 4) As String
I = 0
'将 IP 地址中以 "."为界分成四组十进制数并存入数组
While InStr(temp, ".") > 0
I = I + 1
pts(I) = Mid(temp, 1, InStr(temp, ".") - 1)
temp = Mid(temp, InStr(temp, ".") + 1)
Wend
I = I + 1
pts(I) = temp
'如果 IP 地址中多于 3 个 "."点则转换出错
If I <> 4 Then
AddressStringToLong = 0
Exit Function
End If
'将四组十进制数转换成一个十六进制数
AddressStringToLong = Val("&H" & Right("00" & Hex(pts(4)), 2) & _
Right("00" & Hex(pts(3)), 2) & _
Right("00" & Hex(pts(2)), 2) & _
```

```
Right("00" & Hex(pts(1)), 2))
End Function
```

②利用 SocketsInitialize 函数初始化网络接口. 用 WSAStartup 启动网络, 用 IcmpCreateFile 创建 ICMP 接口.

③利用 IcmpSendEcho (hPort, dwAddress, sData ToSend, Len(sDataToSend), 0, ECHO, Len(ECHO), PING_TIMEOUT)发送 ICMP 数据包, 发送完毕用 IcmpCloseHandle 断开接口, 再用 SocketsCleanup 关闭网络接口.

④用 GetStatusCode 函数接收反馈应答状态, 函数原型为:

```
Public Function GetStatusCode(Status As Long) As String
Dim Msg As String
Select Case Status
Case IP_SUCCESS:
  Msg = "ip success"
Case IP_BUF_TOO_SMALL:
  Msg = "ip buf too_small"
Case IP_DEST_NET_UNREACHABLE:
  Msg = "ip dest net unreachable"
Case IP_DEST_HOST_UNREACHABLE:
  Msg = "ip dest host unreachable"
Case IP_DEST_PROT_UNREACHABLE:
  Msg = "ip dest prot unreachable"
Case IP_DEST_PORT_UNREACHABLE:
  Msg = "ip dest port unreachable"
Case IP_NO_RESOURCES:
  Msg = "ip no resources"
Case IP_BAD_OPTION:
  Msg = "ip bad option"
Case IP_HW_ERROR:
  Msg = "ip hw_error"
Case IP_PACKET_TOO_BIG:
  Msg = "ip packet too_big"
Case IP_REQ_TIMED_OUT:
  Msg = "ip req timed out"
Case IP_BAD_REQ:
  Msg = "ip bad req"
Case IP_BAD_ROUTE:
  Msg = "ip bad route"
Case IP_TTL_EXPIRED_TRANSIT:
  Msg = "ip ttl expired transit"
Case IP_TTL_EXPIRED_REASSEM:
  Msg = "ip ttl expired reassem"
Case IP_PARAM_PROBLEM:
  Msg = "ip param_problem"
Case IP_SOURCE_QUENCH:
  Msg = "ip source quench"
Case IP_OPTION_TOO_BIG:
  Msg = "ip option too_big"
Case IP_BAD_DESTINATION:
  Msg = "ip bad destination"
Case IP_ADDR_DELETED:
  Msg = "ip addr deleted"
Case IP_SPEC_MTU_CHANGE:
  Msg = "ip spec mtu change"
Case IP_MTU_CHANGE:
  Msg = "ip mtu_change"
Case IP_UNLOAD:
  Msg = "ip unload"
Case IP_ADDR_ADDED:
  Msg = "ip addr added"
Case IP_GENERAL_FAILURE:
  Msg = "ip general failure"
Case IP_PENDING:
  Msg = "ip pending"
Case PING_TIMEOUT:
  Msg = "ping timeout"
Case Else:
  Msg = "unknown    msg returned"
End Select
        GetStatusCode = CStr(Status) & "     [ " & Msg & " ]"
End Function
```

在系统调用 GetStatusCode 函数时, 如果反馈应答状态码为 0(Msg = "ip success"), 说明网络正常, 否则网络有故障. 如果反馈状态码为 0 则循环执行①~④步骤进行反复检测.

(3) 反馈状态判断及软件反应

如果反馈应答状态码不为 0, 说明用户设置网络

故障逃避教师机屏幕广播的控制, 弹出网络故障提示窗, 要求用户解除网络故障, 否则 15 秒后注销计算机而不能正常使用.

为了保护 Windows 操作系统的稳定运行, 以 NT 为内核的 Windows 操作系统都运行在保护模式中. 在保护模式中, 在 Win2000 以上的操作系统版本中将指令执行分为三个特权级别, 即 ring0~ring3 权限级别, 但 Win2000 以下的版本没有划分此类权限. Ring0 级是操作系统中执行指令的最高特权, 为 Windows 操作系统本身占用, 可以直接执行诸如访问端口等操作; 而一般的应用程序(如 WORD)等都运行在 ring3 级权限中, 这是级别较低的特权, 不能执行操作系统的底层注销计算机功能, 只使是用程序代码来注销或关闭计算机也不能执行, 本软件也运行在 ring3 级权限中. 在 ring3 级权限中, 如果应用程序确实需要执行系统的底层功能, 必须要提升应用程序的权限才能操作. 在权限提升前首先用 GetVersionEx 判断 Windows 操作系统的版本是否是 NT 内核, 如果是 NT 内核则要提升软件的操作权限才能注销计算机. 提升权限的方法也是调用 Windows API 中的 OpenProcessToken、Lookup PrivilegeValue 和 AdjustToken Privileges 函数来进行. 具体实现为:

```
Public Sub AdjustToken()
Dim lngTokenHandle        As Long
Dim tmpLuid        As LUID
Dim tkp        As TOKEN_PRIVILEGES
Dim tkpTemp        As TOKEN_PRIVILEGES
 ‘打开权限句柄
OpenProcessToken GetCurrentProcess(), (TOKEN_ADJUST_PRIVILEGE Or TOKEN_QUERY), lngTokenHandle
 ‘配置应用程序的权限为特权级
LookupPrivilegeValue"","SeDebugPrivilege",tmpLuid
tkp.PrivilegeCount = 1
tkp.TheLuid = tmpLuid
tkp.Attributes = SE_PRIVILEGE_ENABLED
 ‘提升应用程序的权限为特权级
AdjustTokenPrivileges lngTokenHandle, False, tkp, Len(tkpTemp), tkpTemp, 0
End Sub
```

权限提升主要是通过 AdjustTokenPrivileges 接口使软件从 ring3 提升到 ring0 特权, 只要将软件的操作权限提升到 ring0 级特权, 软件本身就可以用软件代码执行的计算机注销功能.

(4) 热键设置:

软件运行在操作系统的后台, 通过定时器每 2 秒钟发送一次 ICMP 数据包, 系统随机启动后一直执行此操作, 考虑到管理员维护机器的需要或交换机等硬件故障, 应设置取消 ICMP 数据包检测的功能, 使计算机因发生网络硬件故障后也能正常工作, 为此必须在软件内部设置呼出热键, 在上述故障发生时, 通过按下系统热键, 呼出密码输入窗口, 在管理员正确输入密码后取消网线检测功能. 实现方法为通过 SetWindowLong、GetWindowLong、CallWindowProc、RegisterHotKey 和 UnregisterHotKey 函数接口在系统中注册热键消息钩子.

4 结语

系统设计完毕, 通过繁重的代码调试, 软件系统的性能得到了完善与提升. 通过在计算中心 603 实验室中的实时使用, 效果比较明显, 实现了网线在线检测功能, 基本上解决了上课期间学生通过拔除网线或禁用网卡摆脱教师机屏幕广播控制而玩游戏的现象.

参考文献

1 康金辉.数字校园网络主干通讯状态自动测试的设计与实现.计算机系统应用,2011,20(5):113−116,226.

2 王传安,贾丙静,贺文娟,赵海燕.混合 SVM 结合信息熵检测 ICMP 隐通道.计算机应用研究,2010,11:4312−4315.

3 金洪颖,王朝斌,廖鹰梅.校园网网络拓扑发现技术研究.计算机安全,2010,10:43−44.

4 尚建贞 IPv6 下的 ICMP 协议——ICMPv6 浅析.信息系统工程,2010,7:28−29.

5 张金刚,权义宁,赵守凯.运用 Network Coding 改进 IPv6 网络的邻居发现协议.武汉工程大学学报,2010,32(5):94−98.

6 刘震宇,赖粤,王晓红.基于网络处理器的 ICMP 快速处理方法.计算机工程与设计,2010,7:1424−1428.

7 杜树杰.基于 ICMP 协议的 Ping 主机探测.计算机系统应用,2009,18(12):212−214.

8 杨杨,房超,刘辉.ARP 欺骗及 ICMP 重定向攻击技术研究.计算机工程,2008,34(2):103−104,107.