广西科学院学报
Journal of Guangxi Academy of Sciences

2010,26(4):497～499
Vol. 26, No. 4 November 2010

基于 Windows 消息机制的自动检测系统设计
Design of Automatic Test System Based on Windows Messages

赵 钦[1,2],黄 玲[3]
ZHAO Qin[1,2], HUANG Ling[3]

(1.广西大学计算机与电子信息学院,广西南宁 530004;2.广西经济信息中心,广西南宁 530022;3.南宁市红十字会医院,广西南宁 530012)
(1. School of Computer, Electronics and Information, Guangxi University, Nanning, Guangxi, 530004, China; 2. Guangxi Economic Information Center, Nanning, Guangxi, 530022, China; 3. Nanning Red Cross Hospital, Nanning, Guangxi, 530012, China)

摘要:以 Windows 消息机制作为切入点,利用 VC++编程工具设计一个自动检测系统。该系统通过在窗口的过程(WindowProc)获取 Windows 中设备接入、启动、关机等消息并进行分析,对预先想要的消息进行处理,从而有效防止计算机病毒的交叉感染。

关键词:消息机制 检测 系统 交叉感染
中图法分类号:TP316.7,TP271 **文献标识码**:A **文章编号**:1002-7378(2010)04-0497-03

Abstract: Taking Windows Messages as the breakthrough point, the automatic test system is designed by VC++ programming tool. The system, by window proc, obtains and analyzes the information about equipment access, startup, shutdown, etc. The pre-wanted information will be processed to prevent the cross infection of computer virus.

Key words: messages, test, system, cross infection

Windows 应用程序的稳定运行依托消息为核心,在 Windows 中无论是操作系统还是硬件所做的每个动作都会以消息的类型保存,例如设备接入、关机事件等[1]。也就是说当系统触发一种事件时,需要调用操作系统的某种支持,然后操作系统将事件的需要封装成消息,并投入对应的消息队列中,最后应用程序从消息队列中取走消息并进行响应[2]。本文以 Windows 消息机制作为切入点,利用 VC++编程工具设计一个自动检测系统来获取外接设备的接入、计算机关机、启动等消息,以防护计算机不被病毒入侵、篡改和窃取重要信息,从而有效地防止病毒感染计算机,杜绝病毒的交叉感染。

收稿日期:2010-09-21
修回日期:2010-10-27
作者简介:赵 钦(1981-),男,助理工程师,主要从事计算机网络安全和网络存储研究。

1 系统目标

自动检测系统的设计目标是实现以下 4 种功能:(1)实时监控操作系统运行状态,获取"WM_DEVICECHANGE"消息来控制移动存储介质的接入检测和自动调用本地任何程序的运行(如调用杀毒软件对移动存储介质进行查杀);(2)获取"WM_QUERYENDSESSION"关机消息来控制操作系统关机前恢复注册表重要项的数据参数;(3)禁止接入设备的自动运行;(4)实现自动检测系统随操作系统自动启动。

2 系统功能设计

Windows 消息是由一个消息名称(UINT)和两个参数(WPARAM ,LPARAM)组成。消息名称的消息值为 message,该值由<windows.h>内的宏来识别。两个参数(WPARAM ,LPARAM)是一个消息附加参数,信息随 message 的值而改变。

自动检测系统设计原理就是在窗口的过程(WindowProc)中获取消息并进行分析,对预先想要的消息进行处理[3]。

2.1 检测移动存储介质接入及调用本地程序

在Windows操作系统中,当计算机上有设备插入时,将触发Windows的"WM_DEVICECHANGE"消息。自动检测系统利用函数捕获接入设备的各个参数。

利用LRESULT WindowProc(UINT message,WPARAM wParam,LPARAM lParam)检测接入设备的变化。当检测系统获得消息后,对wParam进行判断,如果是DBT_DEVICEARRIVAL发生变化说明有设备已经插入操作系统,然后获取刚插入设备的盘符,并判断插入的设备是否为"DRIVE_REMOVABLE"类型,如果是该类型说明插入的设备是移动存储介质。判断为移动存储介质后,可以根据自定义调用本地的任何程序,包括对移动存储介质的复制、粘贴和调用本地防病毒软件对移动存储介质进行查杀等功能[4,5]。实现这些功能的简单示例代码如下[6]:

```
LRESULT WindowProc(UINT message, WPARAM wParam,LPARAM lParam)
switch(message)
case WM_DEVICECHANGE:
PDEV_BROADCAST_HDR lpdb = (PDEV_BROADCAST_HDR)lParam;
switch(wParam)
case DBT_DEVICEARRIVAL:
  if (lpdb->dbch_devicetype == DBT_DEVTYP_VOLUME)
  {
  PDEV_BROADCAST_VOLUME lpdbv = (PDEV_BROADCAST_VOLUME)lpdb;
  // 获取当前插入设备对应磁盘编号 A--Z
  char chDisk = FirstDriveFromMask(lpdbv->dbcv_unitmask);
  CString strDisk;
  strDisk.Format("%c:\\",chDisk);
  if(CValidFunction::IsPathExist(strDisk))
    UINT nDriveType = GetDriveType((LPCTSTR) strDisk);
  if(nDriveType == DRIVE_REMOVABLE)
  Sleep(500);// 插入设备为可移动设备(U盘或Mp3等)
  调用本地防病毒软件对移动存储系统进行查杀。
  return WindowProc(message, wParam, lParam);
```

获取移动存储介质盘符的方法是利用自定义的函数FirstDriveFromMask来实现,其实现的简单示例代码如下[6]:

```
Char FirstDriveFromMask (ULONG unitmask)
char i;
for (i = 0; i < 26; ++i)
if (unitmask & 0x1)
break;
unitmask = unitmask >> 1;
return (i + 'A');
```

2.2 控制操作系统关机前恢复注册表数据参数

自动检测系统通过获取Windows的"WM_QUERYENDSESSION"关机消息对userinit文件在操作系统注册表中键值项进行数据参数修复,防止病毒对userinit修改后,造成操作系统无法登陆,产生自动注销的现象。userinit还原只是注册表修复功能的一项应用,我们还可以对病毒经常破坏的注册表重要项进行修复,防止在病毒篡改注册表后,造成操作系统无法启动的现象。其实现简单示例代码如下:

```
LRESULT WindowProc(UINT message, WPARAM wParam,LPARAM lParam)
switch(message)
case WM_QUERYENDSESSION:
UpdateData();
if(RegKey.RegOpen(HKEY_LOCAL_MACHINE, REG_LOCAL_USERINIT) == ERROR_SUCCESS)
if(m_bAutoRun)
RegKey.RegWrite(REG_KEY_USERINIT, REG_PATH);
\\ REG_KEY_USERINIT 为注册表中的键值名称,REG_PATH 为注册表中的键值的数据值。
break;
```

2.3 禁止接入设备的自动运行

在自动检测系统界面上设置一个勾选项,针对操作系统注册表中禁止移动介质自动运行的键值数据进行修改,实现禁止接入设备自动运行。其实现

简单示例代码如下:

```
void OnCheckAutorun ()
CRegisterKeyRegKey;
int d1=255;int d2=181;int d3=149;int d4=145;
//d1,d2,d3,d4 注册表中需要修改的键值数据
UpdateData();
if(RegKey. RegOpen(HKEY_LOCAL_MACHINE,REG_LOCAL_NOAUTORUN) == ERROR_SUCCESS)
if(m_bAutoRu)
RegKey. RegWrite(REG_KEY_NoDriveTypeAutoRun, (DWORD&)d1);
else
RegKey. RegDel(REG_KEY_NoDriveTypeAutoRun);
if(RegKey. RegOpen(HKEY_CURRENT_USER,REG_LOCAL_NOAUTORUN) == ERROR_SUCCESS)
if(m_bAutoRu)
RegKey. RegWrite(REG_KEY_NoDriveTypeAutoRun, (DWORD&)d2);
else
RegKey. RegWrite(REG_KEY_NoDriveTypeAutoRun, (DWORD&)d4);
//REG_LOCAL_NOAUTORUN 为注册表中的数据名称路径,REG_KEY_NoDriveTypeAutoRun 为需要修改的键值名称.
```

2.4 实现自动检测系统随操作系统自动启动

在自动检测系统界面上设置一个勾选项,针对操作系统注册表中自动启动的键值数据进行修改,实现自动检测系统随操作系统自动启动。通过函数“GetModuleFileName”来获取自动检测系统在操作系统中存放的完整路径名称,也就是说不管将自动检测系统放在哪个盘哪个文件夹下面,其都会自动检测出自己所在的位置并写入注册表启动项中。其实现简单示例代码如下:

```
Void OnCheckAutorun()
UpdateData();
if(RegKey. RegOpen(HKEY_LOCAL_MACHINE , REG_LOCAL_AUTORUN) == ERROR_SUCCESS)
if(m_bAutoRun)
CString strUDiskExe;
GetModuleFileName ( NULL, strUDiskExe. GetBuffer(MAX_PATH),MAX_PATH);
strUDiskExe. ReleaseBuffer();
RegKey. RegWrite ( REG _ KEY _ RUN, strUDiskExe);
// REG_LOCAL_AUTORUN 为注册表中的数据名称路径,REG_KEY_RUN 为需要修改的键值名称. strUDiskExe 为自动检测系统存放的路径。
```

3 结束语

本文利用 VC++编程工具设计一个自动检测系统,该系统通过利用 Windows 消息机制对自定义的 Windows 消息进行实时监控,实现了控制移动存储介质的接入检测和自动调用本地任何程序的运行、控制操作系统关机前恢复注册表重要项的数据参数、禁止接入设备的自动运行以及自动检测系统随操作系统自动启动等功能,从而自动防护计算机的安全,杜绝了计算机病毒的交叉感染。同时 Windows 消息机制可以在许多自动化的设备上使用,这样可以使得工作人员对这些设备的操作和控制更加的简单、容易。

参考文献:

[1] 王亚,宋铭利. Windows 消息机制研究[J]. 现代计算机,2008,277:70-71.

[2] 廖俊平,马永强,段国兵. 基于 Windows 消息机制的人机交互的研究与应用[J]. 成都信息工程学院学报,2004,19(1):36-39.

[3] 鄢智强,王小峰. Windows 消息机制剖析[J]. 福建电脑,2009(6):24-25.

[4] 俞卫华,路松峰. 移动存储介质信息安全系统的研究与实现[J]. 计算机工程, 2009,35(19):135-140.

[5] 池同柱,陈平. 移动存储介质的信息安全[J]. 科技信息:科学教研, 2008 (25):39-86.

[6] Anthony Jones,Jim Ohlund. windows 网络编程[M]. 第 2 版. 杨合庆,译. 北京:清华大学出版社,2002.

(责任编辑:韦廷宗)