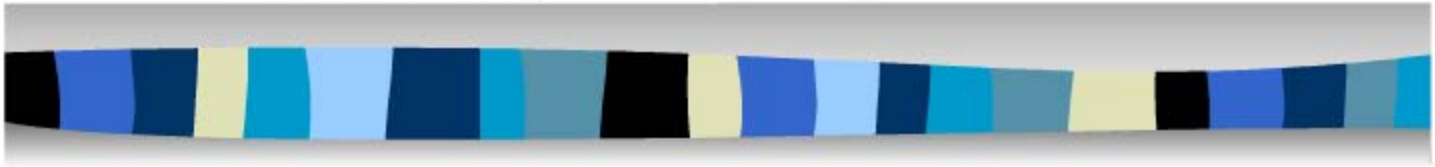
钩子(Hook)



Hook

- 是一种系统消息处理机制，使得应用程序可以安装一个自定义的子过程，以监视系统信息流向，并且对于某些特定的信息，在其到达目标的窗口过程之前，进行一定的处理。

分类

- **Local Hooks**
  - 当前进程中的某一线程
- **Remote Hooks**
  - **Thread** 其它进程中的某一线程
  - **System Wide** 整个系统进程中的所有线程

安装与卸载

- **HHOOK SetWindowsHookEx(int idHook, HOOKPROC hkprc, HINSTANCE hmod, DWORD dwThreadID);**
- **LRESULT WINAPI hkprc (int nCode, WPARAM wParam, LPARAM lParam);**
- **BOOL UnhookWindowsHookEx(HHOOK *hhk*);**

Hook链

- 当许多程序都安装了某种类型的 hook 时，就会形成一个 filter-function chain
- 一旦特定的 event 发生，Windows 会调用该类型中最新挂上的 hook filter function
- LRESULT CallNextHookEx(HHOOK hhook, int nCode, WPARAM wParam, LPARAM lParam);

具体类型

- 1. WH_CALLWNDPROC
  - 每当**SendMessage**发出一条消息到某个窗口时
- 2. WH_CALLWNDPROCRET
  - 每当**SendMessage**发出一条消息后返回时
- 3. WH_GETMESSAGE
  - 每当**GetMessage**或**PeekMessage**从已经挂上**Hook**的线程消息队列取得一条消息时
- **Spy++**

- 4. WH_KEYBOARD
  - 每当**GetMessage**或**PeekMessage**从已经挂上**Hook**的线程消息队列取得一条**WM_KEYDOWN**或**WM_KEYUP**消息时
- 5. WH_MOUSE
  - 每当**GetMessage**或**PeekMessage**从已经挂上**Hook**的线程消息队列取得一条鼠标消息时
- 6. WH_HARDWARE
  - 每当**GetMessage**或**PeekMessage**从已经挂上**Hook**的线程消息队列取得一条硬件（键盘和鼠标除外）消息时（早期**Windows**版本）

- **7. WH_MSGFILTER**
  - 挂上这个**Hook**的线程每当有对话框、菜单或滚动条正要处理一条被**Post**过来的消息时
- **8. WH_SYSMSGFILTER**
  - 任何一个线程每当有对话框、菜单或滚动条正要处理一条被**Post**过来的消息时

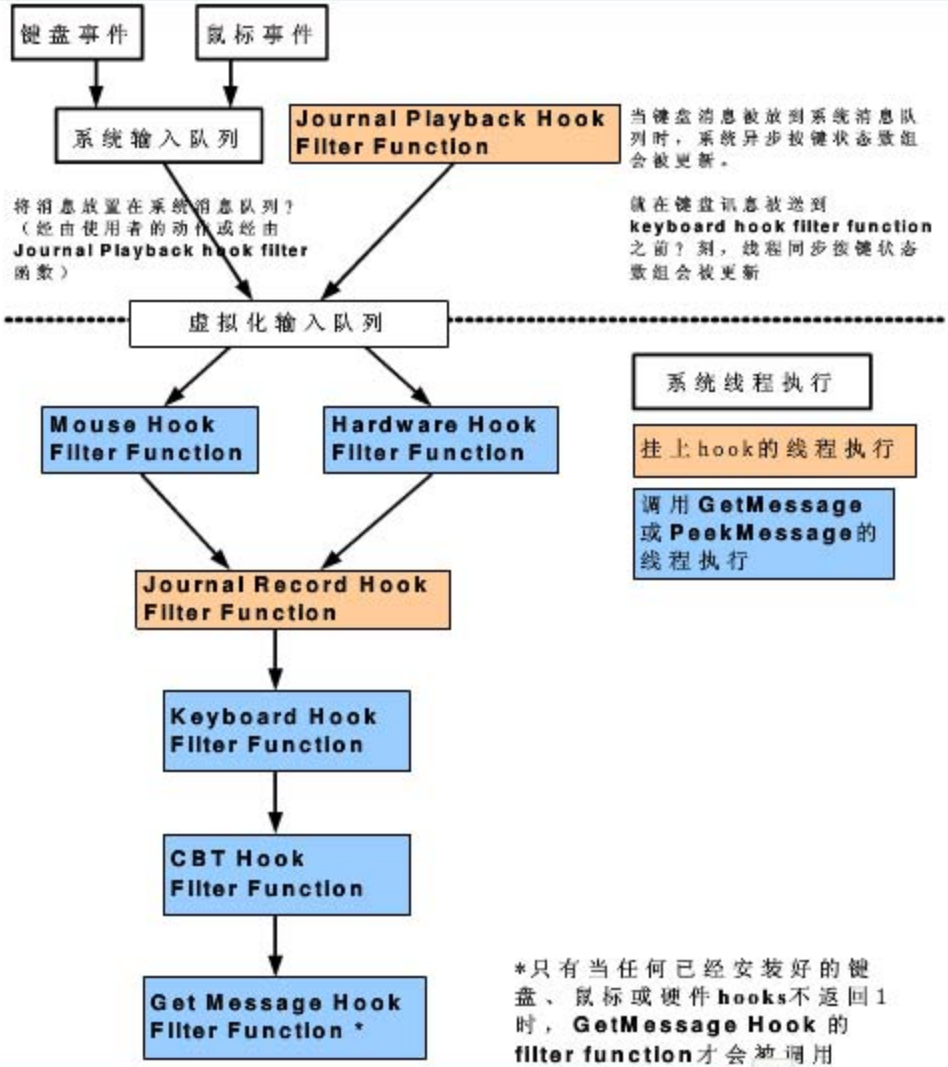
- **9. WH_JOURNALRECORD**
  - 每当有一条消息从系统消息队列中被取出时
- **10. WH_JOURNALPLAYBACK**
  - 每当Windows需要从系统消息队列中提取一条消息时

- 11. WH_SHELL
  - 分五种情况：
  - 只要有一个top-level、unowned窗口被创建、激活或销毁
  - 当任务栏需要重新绘制某个按钮时
  - 当系统需要显示位于任务栏上最小化程序（一个四方形）时
  - 当前键盘布局状态改变时
  - 当用户按下Ctrl+Esc或Alt+Esc时

- 12. WH_CBT
  - 一共有4种情况
  - 每当有一个窗口被创建、激活、最大化、最小化、移动、改变大小
  - 在完成system command 之前
  - 在从system’s hardware input queue中取走鼠标或键盘的事件之前
  - 在设定输入焦点，或取得WM_QUEUESYNC 消息之前

- 13. WH_FOREGROUNDIDLE
  - 当前台线程调用GetMessage函数并且队列中没有消息，即将进入睡眠状态时
- 14. WH_DEBUG
  - 每当任何一个hook filter function 被调用时

- **15.WH_KEYBOARD_LL**
  - 监视输入到线程消息队列中的键盘消息，即当键盘消息将要被投递到线程消息队列之前
- **16.WH_MOUSE_LL**
  - 监视输入到线程消息队列中的鼠标消息，即当鼠标消息将要被投递到线程消息队列之前


键盘事件
鼠标事件
系统输入队列
Journal Playback Hook Filter Function
当键盘消息被放到系统消息队列时，系统异步按键状态数组会被更新。
将消息放置在系统消息队列？（经由使用者的动作或经由 Journal Playback hook filter 函数）
就在键盘讯息被送到 keyboard hook filter function 之前？刻，线程同步按键状态数组会被更新
虚拟化输入队列
系统线程执行
挂上hook的线程执行
调用GetMessage或PeekMessage的线程执行
Mouse Hook Filter Function
Hardware Hook Filter Function
Journal Record Hook Filter Function
Keyboard Hook Filter Function
CBT Hook Filter Function
Get Message Hook Filter Function *
*只有当任何已经安装好的键盘、鼠标或硬件hooks不返回1时，GetMessage Hook 的filter function才会被调用

Hook概览

- Monitor实例
- 源码

KeyBoardHook

- 实例KeyCount
- 源码

SHELLHOOK

- AppLog
- 源码

JOURNAL

- Echo
- 源码
- typedef struct tagEVENTMSG {
    UINT message;
    UINT paramL;
    UINT paramH;
    DWORD time;
    HWND hwnd;
} EVENTMSG, *PEVENTMSG;

鼠标捕捉

- Capture
- 源码

强制发送键盘消息

- SKDemo
- 源码
- 适用于Win2000以前版本