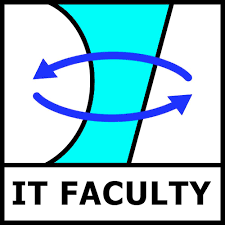


**ĐẠI HỌC ĐÀ NẴNG**

**TRƯỜNG ĐẠI HỌC BÁCH KHOA**

**KHOA CÔNG NGHỆ THÔNG TIN**

----------



***BÁO CÁO ĐỒ ÁN*  
CƠ SỞ NGÀNH MẠNG**

***ĐỀ TÀI***

1. **Tìm hiểu Hook windowns và xây dựng chương trình Keylog**
2. **Tìm hiều Ipv4 và xây dựng chương trình my\_scanip**

**GVHD**: **ThS.** **NGUYỄN THẾ XUÂN LY**

**SVTH**: **Lê Trung Nam**

**MSSV**: **102170036**

***Đà Nẵng****, 2020*

MỞ ĐẦU

Đồ án cơ sở ngành mạng là một trong những đồ án quan trọng của ngành Công Nghệ Thông Tin. Thông qua đồ án này em là người làm đồ án này sẽ đạt được những kiến thức cơ bản, nền tảng và có cơ hội được nghiên cứu chuyên sâu hơn về bộ môn *Lập trình mạng và Nguyên lí hệ điều hành.*

Trong đồ án này, về phần *Nguyên lí hệ điều hành*, đề tài nghiên cứ về Hook windowns và từ đó xây dựng chương trình keylog, còn phần *Lập trình mạng*, đề tài nghiên cứu, tìm hiểu về Ipv4 để rồi viết chương trình my\_scanip. Với sự đồng hành và hỗ trợ nhiệt tình của các thầy cô bộ môn ngành Mạng cùng sự nỗ lực cố gắng của bản thân, bản báo cáo *Đồ án cơ sở ngành mạng* đã hoàn thành đúng với thời hạn được giao.

Đặc biệt em xin trân trọng cảm ơn thầy Nguyễn Thế Xuân Ly đã hướng dẫn và chỉ bảo tận tình trong quá trình em nghiên cứu đồ án này.

***Sinh viên thực hiện***

Lê Trung Nam

MỤC LỤC

[MỞ ĐẦU 2](#_Toc51406153)

[MỤC LỤC 3](#_Toc51406154)

[PHẦN I: NGUYÊN LÝ HỆ ĐIỀU HÀNH 4](#_Toc51406155)

[**1.** **CỞ SỞ LÍ THUYẾT** 4](#_Toc51406156)

[**1.1.** **Hook là gì?** 4](#_Toc51406157)

[**1.2.** **Phân loại Hook** 5](#_Toc51406158)

[**1.3.** **Cách sử dụng** 8](#_Toc51406159)

[**a.** **Cài đặt hook** 8](#_Toc51406160)

[**b.** **Giải phóng Hook** 8](#_Toc51406161)

[**1.4.** **Win 32 API** 9](#_Toc51406162)

[**a.** **Giới thiệu** 9](#_Toc51406163)

[**b.** **Các hàm thường dùng** 9](#_Toc51406164)

# PHẦN I: NGUYÊN LÝ HỆ ĐIỀU HÀNH

**TIÊU ĐỀ: Tìm hiểu về Hook windowns và xây dựng chương trình Keylog**

Yêu cầu đề tài:

1. Giới thiệu Hook windowns, phân loại và cơ chế hoạt động của Hook, cách cài đặt.

2. Viết chương trình Keylog

3. Viết báo cáo theo mẫu Bộ môn mạng và Truyền thông

4. Gặp giáo viên hướng dẫn, làm đúng yêu cầu của giáo viên hướng dẫn và báo cáo tiến độ đúng thời gian

5. Ngôn ngữ dùng để viết chương trình C trên windowns

6. Làm 10 đến 15 slide để bảo vệ sau khi được giáo viên hướng dẫn cho phép.

## **CỞ SỞ LÍ THUYẾT**

## **Hook là gì?**

Hook là một cơ chế trong lập trình sự kiện, cho phép ứng dụng có thể cài đặt một hàm giám sát vào quá trình lưu chuyển các thông điệp. Hay nói cách khác Hook là một cơ chế cho phép chặn các sự kiện (chuột, bàn phím, thông điệp) trước khi chúng được gửi tới hàng đợi của ứng dụng. Hàm dùng để chặn một loại sự kiện riêng biệt được gọi là Hook procedure/ Hook function, khi nhận được sự kiến Hook procedure có thể thay đổi hoặc có thể loại bỏ sự kiện đó.

Hook có khả năng can thiệp rất sâu vào hệ thống, nó có thể làm hệ thống hoạt động chậm chạp hơn hoặc thập chí có thể làm treo hệ thống nếu như xử lý không tốt. Vì thế chúng ta chỉ nên sử dụng Hook trong những trường hợp cần thiết và phải loại bỏ nó khi đã hoàn thành xong công việc.

## **Phân loại Hook**

1. **Phân loại theo phạm vi hoạt động**

* Hook cục bộ (Thread Hook hay loacal Hook): là một kỹ thuật Hook dùng để bẫy sự kiện ngay trong tiến trình cài đặt, hàm giám sát được đặt sau hàng đợi thông điệp ứng dụng.
* Hook toàn cục (Global Hook): hàm giám sát được cài đặt sau hàng đợi thông điệp hệ thống, kiểm soát toàn bộ tiến trình trong hệ thống. Thủ tục hook toàn cục phải được phai báo ở một dll (Dynamic link library) riêng biệt.

1. **Phân loại theo thông điệp xử lý**

|  |  |
| --- | --- |
| **Loại Hook** | **Tác dụng** |
| **WH\_CALLWNDPROC** | Cho phép giám sát các thông điệp được gởi tới một cửa sổ. Hệ thống gọi thủ tục Hook của WH\_CALLWNDPROC trước khi gởi thông điệp đến cửa sổ đích và gọi WH\_CALLWNDPROCRET sau khi thủ tục ở cửa sổ đích xử lý xong thông điệp. |
| **WH\_CALLWNDPROCRET** | Hook WH\_CALLWNDPROCRET truyền một con trỏ có cấu trúc CWPRETSTRUCT tới thủ tục Hook. Cấu trúc này chứa giá trị trả về của thủ tục cửa sổ đã xử lý thông điệp |
| **WH\_CBT** | Windows gọi hàm Hook\_CBT trước khi tạo lập, kích hoạt, huỷ, thu nhỏ, phóng to, di chuyển, thay đổi kích thước, ... của sửa sổ giao diện, hoặc trước khi huỷ bỏ một sự kiển chuột hay bàn phím khỏi hàng đợi của hệ thống, hoặc trước khi đặt một điều khiển vào một input nào đó; hoặc trong lúc đồng bộ hàng đợi thông điệp hệ thống. Giá trị trả về của thủ tục Hook cho biết hệ thống sẽ chấp nhận hay la huỷ bỏ những hành động đó hay không. Hook WH\_BCT thường được dùng cho chương trình đào tạo trên máy tính. |
| **WH\_DEBUG** | Hệ thống gọi thủ tục WH\_DEBUG trước khi gọi các thủ hook tục khác trong hệ thống. Ta có thể dùng hook này để xác định xem có cho phép các thủ tục hook khác hay không. |
| **WH\_FOREGROUNDIDLE** | Hook này cho phép ta thực thi các tác vụ với mức ưu tiên thấp khi các tiến trình chạy nền của nó được đặt ở trạng thái nghỉ. Hệ thống gọi thủ tục WH\_FORGETGROUNDIDLE khi chương trình chạy nền chuẩn bị chuyển sang chế độ nghỉ ngơi. |
| **WH\_GETMESSAGE** | Hook này cho phép một chương trình giám sát các thông điệp được trả về bởi các hàm GetMessage và PeekMessage. Ta có thể dùng hook WH\_GETMESSAGE để giám sát sự kiện chuột và bàn phím và các sự kiện khác được gửi đến hàng đợi thông điệp. |
| **WH\_JOURNALPLAYBACK** | Cho phép chèn chương trình chèn thông điệp vào hàng đợi của hệ thống. Ta có thể dùng hook này để chạy lại (play back) các sự kiện chuột, bàn phím được ghi lại bởi hook WH\_JOURNALRECORD. Khi hook WH\_JOURNALPLAYBACK được cài đặt, chuột, bàn phím sẽ bị đóng băng. Hook này chỉ dành riêng cho hook hệ thống, ta không thể dùng để cài đặt hook cục bộ. Trả về một giá trị time-out, giá trị này cho hệ thống biết phải chờ bao lâu trước khi xử lý thông điệp hiện tại nhận được từ hook WH\_JOURNALPLAYBACK. Điều này cho phép hook có thể điều khiển thời gian của sự kiện mà nó play back. |
| **WH\_JOURNALRECORD** | Cho phép giám sát và ghi lại các sự kiện vào (input event). Hook này thường được dùng để ghi lại chuỗi các sự kiện chuột và bàn phím để sau đó được phát lại nhờ hook WH\_JOURNALPLAYBACKHOOK. Hook này chỉ dành riêng để hook hệ thống, ta không thể dùng để cài đặt hook cục bộ. |
| **WH\_KEYBOARD\_LL** | Cho phép giám sát sự kiện vào của bàn phím được gửi tới hàng đợi ứng dụng. |
| **WH\_KEYBOARD** | Cho phép giám sát thông điệp từ bàn phím WH\_KEYDOWN, WM\_KEYUP |
| **WH\_MOUSE\_LL** | Cho phép giám sát sự kiện vào của chuột được gửi tới hàng đợi ứng dụng. |
| **WH\_MOUSE** | Cho phép giám sát thông điệp của chuột được trả về bởi hàm GetMessage hoặc PeekMessage. Ta có thể dùng hàm này để theo giõi sự kiện nhập từ chuột được gửi đến hàng đợi thông điệp. |
| **WH\_MSGFILTER** | Xử lý hoặc thay đổi tất cả các thông điệp cho hộp thoại cửa sổ, hộp thoại thông điệp hoặc là menu của chương trình |
| **WH\_SYSMSGFILTER** | Xử lý hoặc thay đổi tất cả các thông điệp cho hộp thoại cửa sổ, hộp thoại thông điệp hoặc là menu của hệ thống. |
| **WH\_SHELL** | Một chương trình shell có thể dùng hook WH\_SHELL để nhận các thông báo quan trọng. Hệ thống gọi một thủ tục WH\_SHELL khi chương trình shell được kích hoạt và khi một cửa sổ mức cao (top-level) được khởi tạo hoặc huỷ bỏ. |

## **Cách sử dụng**

## **Cài đặt hook**

Bằng việc gọi hàm **SetWindowsHookEx** sẽ cài đặt thủ tục Hook vào điểm bắt đầu của chuỗi Hook, việc cài đặt Hook có thể được thực hiện trên mọi tiến trình trên hệ thống.

Nếu chúng ta muốn sử dụng Hook toàn cục thì cần phải đặt trong thư viện liên kết động (dll).

Để sử dụng thư viện liên kết động thì phải lấy được handle của thư viện đó, để nhận handle chúng ta có thể sử dụng hàm **LoadLibrary** với tham số là tên của thư viện. Khi có được Handle tiếp đến lấy địa chỉ của thủ tục Hook trong DLL bằng cách sử dụng hàm **GetProcAddress.** Sau khi đã có địa chỉ thủ tục Hook cuối cùng ta sẽ dùng hàm **SetWindowsHookEx** để cài đặt thủ tục Hook vào chuỗi Hook.

HHOOK SetWindowsHookExA (

int idHook,

HOOKPROC lpfn,

HINSTANCE hmod,

DWORD dwThreadId

);

Trong đó:

* **idHook**: là loại thủ tục được cài đặt
* **Ipfn**: con trỏ tới thủ tục Hook
* **hMod**: Handle đến file dll chứa thủ tục Hook chỉ bởi con trỏ Ipfn
* **dwThreadId**: đinh danh Thread mà thủ tục Hook được liên kết, nếu bằng 0 thì Hook sẽ là Gloabal.

## **Giải phóng Hook**

Để loại bỏ Hook chúng ta sẽ sử dụng hàm **UnhookWindowsHookEx.**

Với Hook Global thì hàm này không thể trả tự do cho hàm DLL

## **Win 32 API**

## **Giới thiệu**

Đây là bộ giao diện lập trình ứng dụng (API) cốt lõi của Microsoft có sẵn trong hệ điều hành Windows. Công cụ hỗ trợ phát triển có sẵn trong cái phiên bản của Microsoft Windows SDK, cung cấp tài liệu cà các công cụ cần thiết để xây dựng phần mềm dựa trên giao diện API Windows và các Windows được liên kết.

API Windows (Win32) tập trung chủ yếu vào ngôn ngữ lập trình C ở chỗ các chức năng và cấu trúc dữ liệu được hiển thị của nó được mô tả bằng ngôn ngữ đó. Tuy nhiên, các API có thể sử dụng bởi bất kỳ ngôn ngữ lập trình biên dịch.

## **Các hàm thường dùng**

* **SetWindownsHookExA**

HHOOK SetWindowsHookExA (

int idHook,

HOOKPROC lpfn,

HINSTANCE hmod,

DWORD dwThreadId

);

Trong đó:

* **idHook**: là loại thủ tục được cài đặt
* **Ipfn**: con trỏ tới thủ tục Hook
* **Ipfn**: con trỏ tới thủ tục Hook
* **hMod**: Handle đến file dll chứa thủ tục Hook chỉ bởi con trỏ Ipfn
* **dwThreadId**: đinh danh Thread mà thủ tục Hook được liên kết, nếu bằng 0 thì Hook sẽ là Gloabal.
* **UnhookWindownHookEx**

BOOL UnhookWinowsHookEx (

HHOOK hhk

);

Trong đó:

* **hhk**: Xử lý hook được gỡ, tham số này là một handle của hook lấy được khi gọi hàm SetWindowsHookExA ở trước.
* **CallNextHookEx**

LRSULT CallNextHookEx (

HOOK hhk,

Int nCode,

WPARAM wParam,

LPARAM lParam

);

Trong đó:

* **hhk:** bỏ qua tham số này điền null
* **nCode:** Mã Hook được truyền vào hàm thủ tục Hook hiện tại, thủ tục Hook tiếp theo sử dụng tham số này để biết cách xử lý.
* **wParam:** Giá trị wParam được truyền vào thủ tục Hook hiện tại. Ý nghĩa của tham số này phụ thuộc vào loại Hook liên quan với các dây chuyền Hook hiện tại.
* **lParam:** Giá trị lParam được truyền vào thủ tục Hook hiện tại. Ý nghĩa của tham số này này phụ thuộc vào loại Hook liên quan với các dây chuyền Hook hiện tại.
* **LowLevelKeyboardProc**

LRESULT CALLBACK LowLevelKeyboardProc (

\_In\_ int nCode,

\_In\_ WPARAM wParam,

\_In\_ LPARAM lParam

);

Trong đó:

* **nCode**: mã thủ tục của Hook, dùng để xác định thông điệp
* **wParam**: định danh của thông điệp ban phím
* **lParam**: con trỏ đến cấu trúc **KBDLLHOOKSTRUCT**:

***typedef struct tagKBDLLHOOKSTRUCT {***

***DWORD*** *vkCode;*

***DWORD*** *scanCode;*

***DWORD*** *flags;*

***DWORD*** *time;*

***ULONG\_PTR*** *dwExtraInfo;*

***}*** *KBDLLHOOKSTRUCT, \*LPKBDLLHOOKSTRUCT, \*PKBDLLHOOKSTRUCT;*

Trong đó:

* **vkCode**: mã bàn phím ảo, có giá trị từ 1 đến 254
* **scanCode**: mã quét phần cứng của bàn phím
* **flags**: để kiểm tra giá trị tổ hơp các phím
* **time**: thời gian chạy thôn điệp này
* **dwExraInfo**: thông tin bổ sung liên quan đến thông điệp
* **GetKeyState**

Lấy trạng thái của phím ảo được chỉ định, trả về 1 là xuống, còn 0 là lên.

SHORT GetKeyState (

Int nVirtKey

);

* **GetKeyboardState**

Sao chép tình trạng của 256 phím ảo đến bộ đệm chỉ định

BOOL GetKeyboardState (

PBYTE lpKeyState

);

* **ToAscii**

Dịch mã phím ảo và trạng thái bàn phím được chỉ định sang ký tự hoặc các ký tự tương ứng

int ToAscii (

UINT uVirtKey,

UINT uScanCode,

const BYTE \*lpKeyState,

LPWORD lpChar,

UINT uFlags

);

Trong đó:

* **uVirtKey**: mã phím ảo cần dịch
* **uScanCode**: mã quét phần cứng của phím cần dịch
* **lpKeyState**: con trỏ đến 1 mảng 256-byte chứa các trạng thái bàn phím hiện tại
* **lpChar**: Bộ đệm nhận ký tự hoặc các ký tự đã dịch.
* **uFlags**: Tham số này phải là 1 nếu một menu đang hoạt động, hoặc 0 nếu không.
* **LoadLibraryA**

Tải module được chỉ định vào không gian địa chỉ của tiến trình gọi. Module được chỉ định có thể làm cho các module khác được tải.

HMODULE LoadLibraryA (

LPCSTR lpLibFileName

);

Trong đó:

* **lpLibFileName**: tên của module, có thể là tên của thư viện (.dll) hoặc module thi hành (.exe). Tên chỉ định là tên của tập tin của module và không liên quan tên chứa trong module. Xác định trong từ khoá thư viện tập tin (.def)
* **GetProcAddress**

Truy xuất địa chỉ của một hàm hoặc biến đã xuất từ ​​thư viện liên kết động (dll) được chỉ định.

FARPROC GetProcAddress (

HMODULE hModule,

LPCSTR lpProcName

);

Trong đó:

* **hModule**: handle của thư viện dll chứa hàm hoặc biến. Handle này là giá trị trả về của các hàm LoadLibrary, LoadLibraryEx, LoadPackageLibrary hoặc GetModuleHandle.
* **lpProcName**: Tên hàm hoặc biến hoặc giá trị thứ tự của hàm. Nếu tham số này là một giá trị thứ tự, nó phải ở từ bậc thấp; từ bậc cao phải bằng 0.

1. **PHÂN TÍNH VÀ THIẾT KẾ HỆ THỐNG**
2. **PHÂN TÍCH YÊU CẦU**
3. **Yêu cầu chức năng**

Chương trình sẽ ghi lại toàn bộ thao tác bàn phím của người dùng máy tính và lưu lại trong một tập tin (.txt)

1. **Yêu cầu về giao diện**

Vì đây là một chương trình có tính chất gián điệp nên sẽ không có đồ hoạ, để biết được chương trính có chạy hay không người dùng có thể xem trong task manager.

1. **Yêu cầu về tương thích**

Do Win 32 API hỗ trợ tốt trên ngôn ngữ C/C++ nên em lựa chọn ngôn ngữ C++ để viết chương trình, công cụ sử dụng là DevC và Visual Studio Code.

1. **PHÂN TÍCH CHỨC NĂNG**
2. **XÂY DỰNG CHƯƠNG TRÌNH**