電腦安全 project2 by 9817059李揚

Code explanation:

這次作業我主要是利用wparam和lparam去完成。

wparam:

wparam是 [**WM\_KEYDOWN**](http://msdn.microsoft.com/en-us/library/windows/desktop/ms646280(v=vs.85).aspx),[**WM\_KEYUP**](http://msdn.microsoft.com/en-us/library/windows/desktop/ms646281(v=vs.85).aspx),[**WM\_SYSKEYDOWN**](http://msdn.microsoft.com/en-us/library/windows/desktop/ms646286(v=vs.85).aspx), or[**WM\_SYSKEYUP**](http://msdn.microsoft.com/en-us/library/windows/desktop/ms646287(v=vs.85).aspx).的其中一個，看狀態決定。而這四個其實分別是256,257,260,261。當按的不是system key且是壓住狀態的話會是WM\_KEYDOWN，不是system key，而壓住後放開會是WM\_KEYUP，是system key壓住狀態會回傳WM\_SYSKEYDOWN，壓住後放開會回傳WM\_SYSKEYUP。根據我的測試，所謂的不是system key是沒有壓住alt鍵的狀態。

而我使用的是WM\_KEYDOWN。因為實際上我在電腦打字的時候若A很久是會出現很多A的。且我上網測試過，一般登入軟體輸入密碼時也是如此，所以我預防有人密碼是AAAA這種情形，若用WM\_KEYUP就會記成A，所以我覺得用WM\_KEYDOWN比較合理。

lparam: 是一個指標指到 KBDLLHOOKSTRUCT的資料結構。這資料結構可以幫我們紀錄我們按的是鍵盤上的哪一個鍵，而我可以藉由access裡面的scanCode或vkCode來判斷到底是按哪一個鍵。

scanCode是實際上keyboard傳給電腦的number，以告知電腦室按下哪個鍵。

vkCode是virtual-key code，有鑑於各地文化不同，設計出來的鍵盤可能有所不同，為了解決此問題，視窗作業系統是先讀進scan code在把他轉成virtual key code，然後再根據此virtual key code 做相對應的操作。

不過在撰寫程式的時候去記這些代碼就實在太不方便了，所以在winuser.h檔裡有去define。如: #define VK\_CONTROL 17。

而這次作業我選擇用vkCode來實作，因為我發現在數字0~9還有A-Z方面他回傳的值恰巧跟ASCII code裡的0~9和大寫的A-Z是一模一樣的，恰巧符合作業要求，所以我就只需要把它們當作char印到筆記本上即可，不用做太多的轉換。

What I can do using API hooking:

可以做即時翻譯軟體。在打出本文之前，就用hook的方法偷偷執行我想要做翻譯的程式，如此一來就可以達到即時翻譯的效果。實際上Hook TextOut(), ExtTextOut()就是可以實作此效果的函式。

Other way to hook API:

自己寫一段程式碼，讓他達到hook效果。

Ex:

現在有一程式碼為:

…

-------------🡪想在這裡hook

…

我就加上這些程式碼

…

pushad

the thing I want to do

popad

…

如此一來就達到hook的效果了。

PS: 實際上，這些因為機械碼，不過我以組合語言方式表示。只要把這些指令換成機械碼即可。