國立台北大學資訊工程學系專題報告

SECRET KEY

專題組員:賴柏恩、王祐晨

專題編號：PRJ-NTPUCSIE-104-3
執行期間：104 年 9 月 至 105 年 6 月

1. 簡介

最近的巴拿馬文件事件、LINE 勒索軟體 Cryptolocker 的出現，使我們不能再忽視資訊安全的問題。為了維護商業機密的安全，市面上已有一種非常實用的加密工具叫加密碟，提供電腦或儲存媒體遺失或遭竊時的加密保護，利用加密碟內建的程式與晶片進行加密，將軟體加密的缺點徹底解決，確保未經授權的使用者無法看到任何資料。

但市售的加密碟仍然有問題存在，為此本專題設計了一套全新的系統，期望能改善加密碟的缺失。

2. 摘要

加密碟在加密方面固然實用，但是我們還是歸納出幾個缺點：

(1)對於現代人來說，要隨身攜帶加密碟是一件很麻煩的事，再加上體積小，更容易造成遺失。

(2)加密碟的加密動作，必須將加密碟插入電腦中才可執行，可以說是引狼入室。只要被看到加密碟或加密後的資料，就會讓人質疑你的電腦是否有機密文件，就算加密過，還是有資料外洩的危險性存在。

3. 專題進行方式

i. 程式目的

因此我們在思考，究竟要用什麼方法，才能把整個加密過程隱形，不要被別人發現加密的動作或是被加密的資料。這正是我們此支程式的目的，希望能夠改善加密碟的缺點，成為一個能夠取代加密碟的程式。

ii. 進行方式

大家都知道魔術師在變魔術的時候，不管是隔空取物、或是憑空變出東西，都一定有用魔術道具、也就是所謂的媒介。加密碟也是一個媒介，但是我們剛剛討論過，加密碟的缺點就是過於明顯。那究竟要用什麼樣的媒介，才能讓加密的過程隱形呢?

我們就想到，現在這個人手一機的時代，如果利用手機當作媒介。好比說今天我使用完了一個機密資料，我想要隱藏它，但是又不想被發現，這時如果把手機當作鑰匙，手機拿離開電腦，就將資料隱藏，如果又要用這個檔案，只要手機靠近電腦，檔案就會出來。這樣是不是就可以利用手機，達到加密過程隱形。

iii. 程式功能

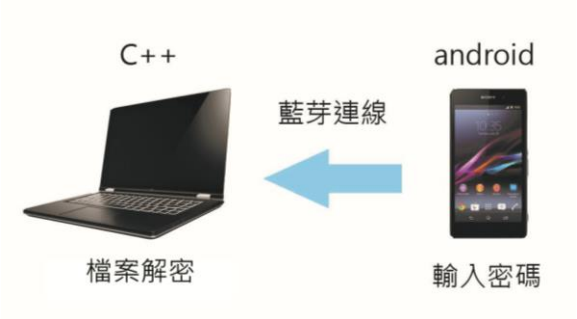
為了取代加密碟，我們將我們的程式設計為兩大功能，第一個功能，

手機靠近電腦，立即對磁碟掛載（圖 1）。

如果使用者認為，只隱藏磁區不夠安全，可以使用我們第二個功能，手機靠近電腦後，利用 APP 輸入密碼，將加密的資料解密(圖 2)。

(圖 1)隱密性模式

(圖 2)安全性模式



iv. 系統實作

1.實作平台

電腦端的程式，是用 C 語言再搭配 C#的介面。手機端的程式，是用 Android Studio。

2.藍芽技術

為了使加密動作看不見，我們使用了手機與電腦的藍芽技術，讓電腦遠端監看、配對使用者的手機藍芽裝置，並將訊號當作鑰匙，結合隱藏磁碟以及檔案加密。

3.檔案加密

在檔案加密的部分，我們利用串流密碼的方式，將使用者選擇的檔案或檔案夾，每個 BIT 做 XOR，並且將檔案路徑存成我們自訂的形式，在解密時透過檔案路徑來還原。

使用者如果輸入密碼要求檔案解鎖時，此時會進行 Challenge and Response 的驗證，必須通過驗證才可以將檔案解密。

Challenge and Response 是為了預防被他人側錄密碼。如果有人側錄並且盜用一般的密碼字串並傳送給電腦，就可以破解解密取得檔案，但如果傳送的只是一串電腦產生的亂數以及雜湊值，就算被竊聽，別人也無法解密我們的檔案。

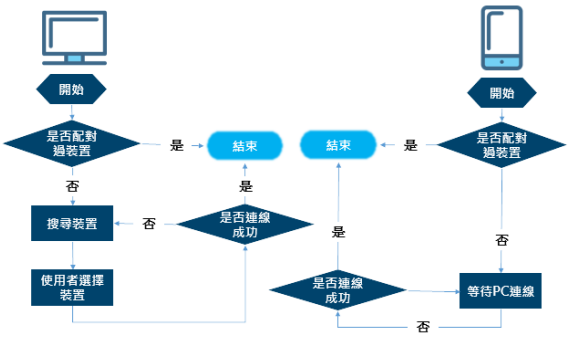
Challenge and Response 的過程為，一開始手機輸入密碼要求電腦開鎖，此時電腦會傳送一個亂數 Challenge 手機，接著手機端與電腦端，兩邊都會利用此亂數與密碼進行”hash function”，雜湊函式是使用 MD5 訊息摘要演算法，手機端將雜湊值 Response 至電腦端，如果雜湊值一致，代表通過驗證。

4.磁碟隱藏

為了只求快速以及隱密性的使用者，我們添加了磁碟隱藏的功能，程式透過 Comment Line 發送指令，利用作業系統，執行掛載與卸載磁碟的動作。

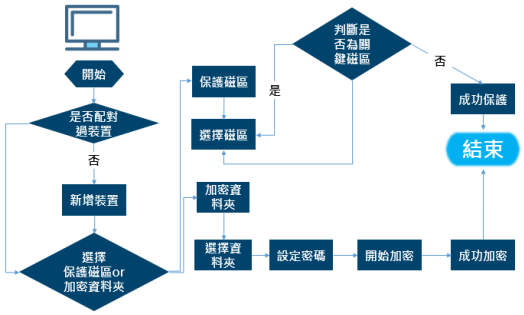
v. 系統流程

1. 新增使用者流程



一開始電腦與手機端會偵測是否配對到藍芽裝置，如果沒有，則 PC 端會搜尋裝置，手機端會等待 PC 連線，再來如果連線成功就進行下個流程，反之則會繼續搜尋裝置與尋找裝置。

2. 隱藏、加密流程

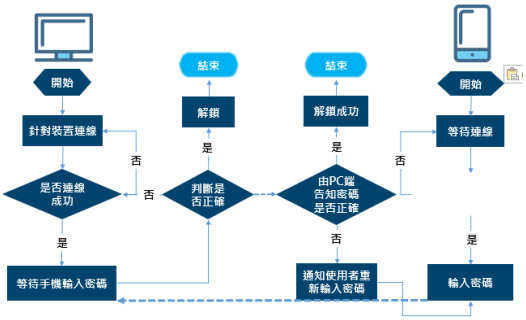


如果 PC 端以配對過藍芽裝置，使用者可以進行選擇模式階段。

若選擇的是隱密性模式保護詞曲，接著讓使用者選擇想要保護的磁區，並且會要求使用者選擇 CDE 槽之外的磁區。

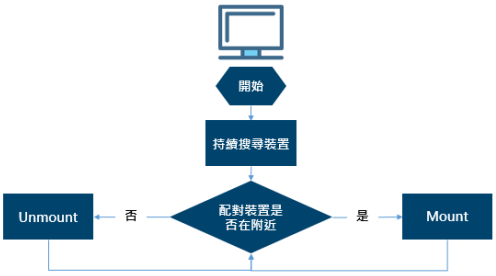
如果使用者選擇的是安全性模式，也就是加密資料夾的話，要求使用者選擇資料夾、設定密碼，設定完後即家開始加密。

3. 檔案解密流程



電腦端會等待輸入密碼，並利用手機 APP 輸入密碼，此時密碼會以藍芽的方式傳到電腦，電腦會判斷是否為正確密碼，並把結果告知手機端，如果輸入錯誤，則手機端要求使用者再次輸入密碼，若輸入正確，就可以成功解鎖。

4. 磁碟隱藏流程



電腦端會持續搜尋綁定的藍芽裝置，如果有看到使用者裝置，則將磁碟掛載(顯現)，若沒有，則將磁碟卸載(隱藏)。

4. 主要成果與評估

i. 研製成果

本專題已達到預期之目的：利用手機，改善了加密碟的缺點，取代加密碟，只要用手機靠近電腦，檔案就會出現，反之檔案就會消失。並且也實踐了另一個功能，利用手機 APP 輸入密碼，檔案即可解密。

ii. 系統介面

iii. 未來可能之擴展方向

未來期望能夠將此概念普及化，並且可以結合雲端或是穿戴式裝置，提供使用者更多元的加密方法。

5. 結語與展望

這次專題真是一個難得的機會，剛從大一、大二學到關於程式設計的知識，馬上在大三學以致用，讓我對於各個課程有更深刻的印象，雖然在製作專題的過程當中，遇到了許多的困難，但我們並沒有因此而氣餒，透過一次次的修改、更新、查詢資料，終於完成這支程式。人常說讀萬卷書不如行萬里路，我們應當做中學才能提高吸收知識的效率。

加密碟因為可以簡單、輕鬆地保護電腦資料，在企業、公司中非常廣泛使用。我們設計出了改善加密碟缺點的程式，若將此程式推廣並且普及到加密市場甚至是一般人的生活中，想必商機一定無可限量。

6. 銘謝

感謝在這一路上幫助我們的人，不管是指導老師、實驗室的學長或是系上同學，你們的幫助與建議，是我們成長的基石，沒有你們的鼓勵就沒有今天的 SECERT KEY。還要感謝專題夥伴之間的互相照應，我們這一年來的辛勞與堅持，在這走到終點的一刻化為豐收的果實，最後再次感謝在這次專題中支持我們的所有人。

7. 參考文獻

[1]https://32feet.codeplex.com/

[2]http://www.ithome.com.tw/article/86742

[3]https://en.wikipedia.org/wiki/List_of_Bluetooth_profiles

[4]https://www.bluetooth.com/develop-with-bluetooth/white-papers