

行動裝置防肩窺攻擊之密碼輸入機制

系所／電腦與通訊工程學系

指導老師／羅嘉寧

組員／邱輝展、連秀慈、夏庭儀、蔣劭廷

智慧型手機中，系統常用的身分認證存有一大難題，就是肩窺攻擊；像是個人身分識別碼、安卓系統螢幕圖形鎖，攻擊者只要直接觀看便能取得使用者密碼，加以惡意使用。

為了防止有意偷窺者，輕鬆地達到目的，使用者能在驗證時加入混淆訊息，使攻擊者無法察覺，導致攻擊者在記錄驗證的過程，無法得知使用者正確的密碼。

本研究希望使用者面臨肩窺攻擊之威脅時，能夠在輸入機密資料的同時，混淆攻擊者。當我們無法躲避他人的視線時，可以藉由使用者本身輸入密碼的習慣，使得攻擊者所肩窺得知之資訊，非實際輸入之資訊，來混淆攻擊者。

蘋果公司在 iOS 8 系統中，首次開放的第三方鍵盤 Custom Keyboard API(如圖 1)。讓開發者能夠利用這些 API 進行開發，我們使用 Xcode 為軟體開發套件的開發環境(如圖 2)，並使用程式語言 Swift 進程式研究及編寫。

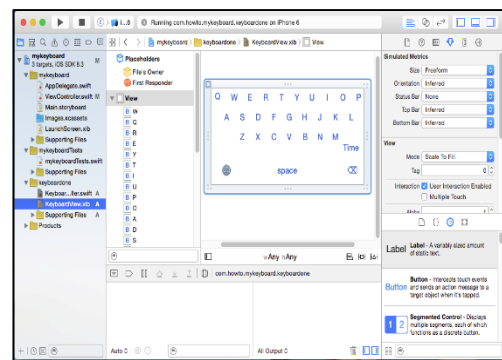


圖 2：本研究的開發環境

我們利用蘋果公司提供的第三方鍵盤 API 做為開發方向，除了官方沒有提供且無法達到的鍵盤功能外(例:長按地球鍵出現輸入法列表、使用浮動框來做自動修正...等)。我們做出一個具有基本輸出功能的自繪鍵盤(如圖 3)，接著使用 Xcode 下所提供的按鈕事件，來製作本研究所需的混淆功能。

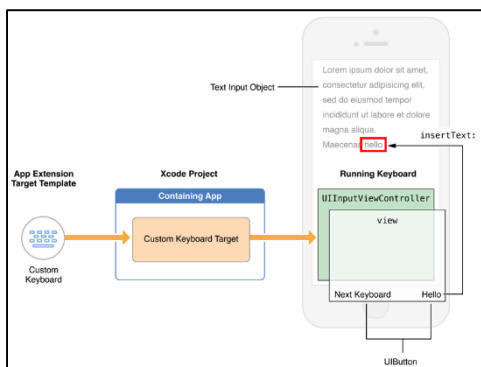


圖 1：第三方鍵盤架構圖(引用)

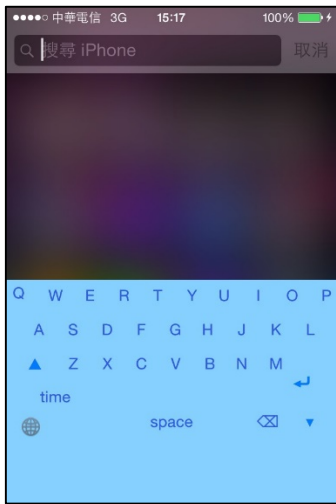


圖 3：手機實測自繪鍵盤畫面

其中我們運用 Touch Down 與 Touch Up 等基本設定，取得不同使用者按下與離開按鈕的時間值，再利用時間差去分析個人的輸入習慣，並且將得到的資訊運用在我們所提供的功能上，達到混淆視覺的目的。

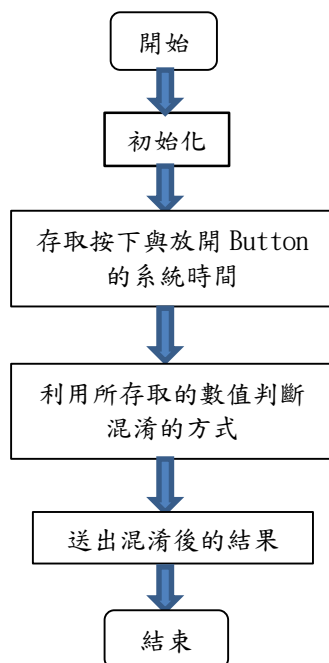


圖 4：輸入程序流程圖

經由以上相關研究與系統研究方法，我們初步研究出幾種混淆視覺上鍵盤輸入的方法且改變了別於一般的輸出方式，希望能達到增加安全及隱密性的鍵盤輸入機制。在個人身分識別與文字密碼解鎖時，多一層防護功能，甚至在被不知情的情況下暴力破解時，也能夠延長攻擊者破解時的時間。