



資訊專題期中 書面報告

組別：NTCU-CS-PRJ-112-13

組員：林家羽、顏岑宇、余宛庭

填寫日期：2022/4/15

一、專題內容製作動機與預期目標

(1) 製作動機：

由於現代網路的發達，無論社交或是工作都跟網路脫不了關係，導致讓想竊取個資的有心人士有跡可循。有心人士可藉由偽裝成使用者欲輸入登入資訊的網站，使其點入該網址，掉入陷阱進而竊取資料。為了預防此現象，我們希望做出一套在在使用上能夠更加安全的 OTP 軟件。

與前一屆的 FudyOTP 相比，前一屆以 AndOTP 為基底開發；而我們使用的是 Aegis Authenticator，在防禦釣魚網站方面前一屆所使用的是 Regular expression 比對 URL，而我們優化 URL 比對的同時，把 URL 傳到 Whois 並提取裡面網站的資訊，更加確保使用者進入的網站不是釣魚網站。

(2) 預期目標：

優化 Aegis Authenticator，增添網址檢查功能及用戶可自行設定安全網址。比對網址方面參考 Bitwarden 的 auto-fill 五種模式，並利用安全分數供使用者參考。在引導介面中設置新手教學，提供使用者更加友善的使用環境。

二、整體時程與工作規劃

工作環節	時程	備註
專題研究方向討論	2 月	
專案環境建置	2~3 月初	
細項工作分配與實行	3 月初~8 月中	附詳細說明
細部調整與測試	8 月中~9 月	

(1) 細項工作分配與實行：

(1) 網址檢查界面製作

1. Layout 樣式設定
2. Component 排版

(2) 網址檢查頁面元件串接

1. 頁面跳轉控制
2. 頁面跳轉回傳參數控制

(3) 網址檢查頁面元件設定及參數調整

1. 元件使用及回傳參數

(4) 網址檢查

1. 建立 Whois Server 資料庫
2. 利用 OTP 金鑰資訊及用戶輸入，建立 URL 比對資料庫
3. Dialog 選項分支及相對應事件處理
4. 解析用戶輸入網址
5. 新增子程序執行網路要求
6. 使用 Whois 抓取網站資訊
7. 將資訊進行中文翻譯
8. 解析翻譯結果，並輸出需要的資訊
9. 測試及 Debug

(5) 新手引導介面

1. 在 menu_main.xml 右上角新增一個 Button
2. 最後一頁增加一個按鈕跳轉 2FA 介紹

3. 2FA 介紹頁面
4. 2FA 介紹的設置
5. 跳轉 2FA 介紹 Button 設置

(6) 書面資料整理及持續追蹤 OTP App 相關資訊

1. 列出 Bitwarden 詳細功能介紹
2. 列出 Aegis 詳細功能介紹
3. 列出上一屆 Fydy App 詳細功能介紹
4. 用 MyOTP App 與上述資料比較

三、經費規劃及使用情形

(1) 購買項目：

Galaxy Tab A7 Lite 4/64(T220)

(2) 採購時程及途徑：

預計採購時程：2022.06

預計採購途徑：網路購買

(3) 用途說明：

開發、實作與測試本專題所設計的具備強化釣魚攻擊抵擋能力之一次性動態密碼（One-Time Password；OTP）系統 — MyOTP，並用以製作專題文件與專題會議記錄。

四、可能遭遇之困難及解決方法

(1) 專題方向的討論及思考創新：

基於市面上有關於的 OTP 的軟體眾多，除了需要一一比較，分析各個 OTP 軟體的優缺點以外，選擇何種軟體作為開發的基底，並思考如何提升安全性及對實用性，分析用戶可能的需求，及對該軟體的深入了和持續追蹤也是一大考驗。

(2) 對於開發環境的不熟悉：

初次接觸 App 程式開發，我們所使用的是 Android Studio。因此，在開發介面的使用及環境建置都必須從零開始學習。

此外，雖然開發過程中使用的是 Java 語言，但是和以前的課程相比，開發過程使用到了以前沒有用過的 Package 及開發 Layout 使用的 XML 等等，都需要上網查資料，閱讀英文文章也成為必備基本能力之一。

(3) 專案從基礎創新：

在原本的 Opensource 中並沒有過多的註解，我們主要工作是在理解 Opensource 原本程式碼及增添額外的功能設定，找到相對應的程式碼並增加內容，若需要新增檔案也需配合原本程式碼的命名原則。