Android 行動裝置隱私衝擊評估系統之實作

陳冠霖
國立高雄師範大學
kuanlin81625@outlook.com

楊中皇
國立高雄師範大學
chung47@gmail.com

摘要

行動裝置通常存放了許多的個人資料，而現今的行動裝置裡廠商預載或者從 Google Play 商店下載下來的應用程式，客戶端必須完全接受該應用程式設定的所有條件才能使用，無形之中，使用者本身儲存在行動裝置裡的個人資料就已經暴露在隱私的風險當中了。本研究主要的目的是探討 Android 作業系統和應用程式的個人資料安全，以及對個人隱私的影響。參照紐西蘭隱私專員辦公室(Office of the Privacy Commissioner)和加拿大科技部(Ministry of Technology, Innovation and Citizens' Services)提出之隱私衝擊評估(Privacy Impact Assessment)相關步驟與方法，描述系統與應用程式擁有的權限內容及收集的資料，透過 Android Logger 分析可能的意圖與活動的行為，進而評估隱私之風險。

關鍵詞：隱私衝擊評估、個人資料、權限、意圖

壹、前言

2014 年全球已經超過 10 億人口正在使用智慧型手機(Gartner 2015)，而 Google 開發的 Android 行動裝置作業系統超過八成的市佔率(IDC 2015)，代表著全球擁有非常龐大數量的 Android 使用者。由於行動裝置本身的特性，通常會存放許多的個人資料，當中包含了大量的個人隱私，然而，市面上許多應用程式開發商為了提供完整的客製化、個人化服務，通常會要求很多的管理權限，例如：位置、聯絡人、通話資訊、讀取與寫入 SD 卡、裝置和應用程式紀錄，等等。Google Play 商店並沒有要求應用程式開發商提供如何使用客戶端的個人資料，以及收集用途和方法，客戶端必須完全接受權限的要求，才能下載安裝。在不知道開發商以及 Android 作業系統本身如何使用個人資料的情況下，不但讓惡意軟體有機可趁，也讓使用者的隱私暴露於風險當中。因此本研究以保護個人隱私資料為出發點，主要目的為探討應用程式以及 Android 作業系統對於個人資料使用的流程，確保個人隱私資料正確的、合法的、非惡意的、經過使用者允許的情況之下被應用程式所使用，同時進一步的檢測是否有潛藏和惡意的行為正在執行或是系統漏洞而導致個人資料的洩漏。

貳、文獻探討

本章節將說明何謂隱私衝擊評估，以及詳細介紹系統實作所探討的議題，對實作過程使用的工具和概念做說明。

一、隱私衝擊評估

隱私衝擊評估可以在專案或系統開發實作的過程當中，有效且系統化的幫助組織和企業去鑑定風險可能存在的位置以及分析個人資料在系統裡如何運作，從而了解系統對於個人隱私造成的影響(Information Commissioner's Office 2014)。在此過程當中，開發者可以使用任何已經存在的分析工具，任何形式的評估方法去實現完整的隱私衝擊評估作業。主要目的就是要將任何可能會影響個人隱私的風險降到最低。根據紐西蘭隱私專員辦公室所提出的手冊，完整的隱私衝擊評估可分為以下三大階段(Office of the Privacy Commissioner 2007)。

（一）初步隱私分析：評估此專案或計畫是否需要進行完整的隱私評估。

（二）隱私衝擊評估：完整描述專案或計畫的內容，包括如何使用、存放、修改、傳輸個人資料，然後對此進行評估。

（三）隱私衝擊報告：將以上所有過程詳細的紀錄且製作成報表(圖 1)。

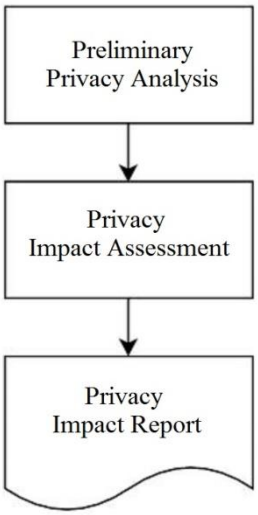

圖 1：隱私衝擊評估三大階段

依照第一階段的前階評估來決定是否進行完整的隱私評估，若是需要，則繼續進行第二階段—隱私衝擊評估，此階段可再細分為以下六步驟。

（一）介紹與總覽(Introduction and Overview)

首先，一份完整的隱私衝擊評估必須要淺顯易懂，用字遣詞盡量平易近人，才能夠供老闆、主管、股東、沒有資訊科學背景的人閱讀。再來必須解釋進行隱私衝擊評估的原因，介紹分析的架構，以及其他跟隱私相關的細節。

（二）描述與定義(Description and Define)

決定實行隱私衝擊評估的範圍以及對象，定義何謂個人隱私資料，描述系統或是應用程式專案所使用的個人隱私資料。若根據加拿大科技部對個人資料的定義，除了直接可以與人聯結在一起的聯絡資料，所有可以識別個人的資訊都算是個人資料的一部份，例如：姓名、年齡、性別、血型、信仰、家庭狀況、經濟狀況、教育程度、健保紀錄、犯罪紀錄、工作經驗、個人發表意見，等等(Ministry of Technology 2014)。

（三）隱私分析(Privacy Analysis)

隱私分析遵照資料的「生命週期」，從取得、保存、使用、處理、分享、傳

輸到刪除，必須清楚的解釋系統或應用程式取得了哪些資料，用什麼方法取得，為什麼要收集，獲得個人資料之後存放在哪些地方，系統開發者會如何使用以及處理這些資料，過程中是否會將資料分享給其他應用程式，甚至傳輸至其他企業、地區、國家的伺服器儲存。

（四）風險評估(Risk Assessment)

以使用者、客戶端的角度對隱私可能受影響的方式、類型與程度作更詳細的判斷，根據先前對資料的定義和隱私的分析，釐清使用者可能感到擔心甚至產生疑慮的行為，評估資訊流動的方向與過程對個人隱私造成的影響程度。

（五）加強措施(Enhancing Response)

依據三、四步驟分析評估的結果，對系統或應用程式進行加強措施，填補漏洞、修正設定、精進效能，以達到隱私衝擊評估最終目標－將任何可能會影響個人隱私的風險降到最低。

（六）結果報告(Conclusion)

總結需要視各企業組織的需求或是原先目標，說明此評估的執行的情況以及重要貢獻，然後列舉相關辦法、適用的法律規範、商業政策、相關範例或是其他可參考之經驗，提供老闆、主管和股東做為未來隱私策略之依據。

二、Android Logger

透過分析系統的 Log，可以獲得相當多的錯誤訊息和警告訊息，甚至是重要資訊，通常可以用來解決一些致命且複雜的問題(Yaghmour 2013)。Android 核心提供了四種 Log 型態，分別為：main、radio、event 和 system。同時也支援 logcat 指令，可以透過 ADB 或是直接在 Shell 裡面查看 Log 紀錄的內容(Drake et al. 2014)。概略的 Android Log 系統如圖 2 所示。

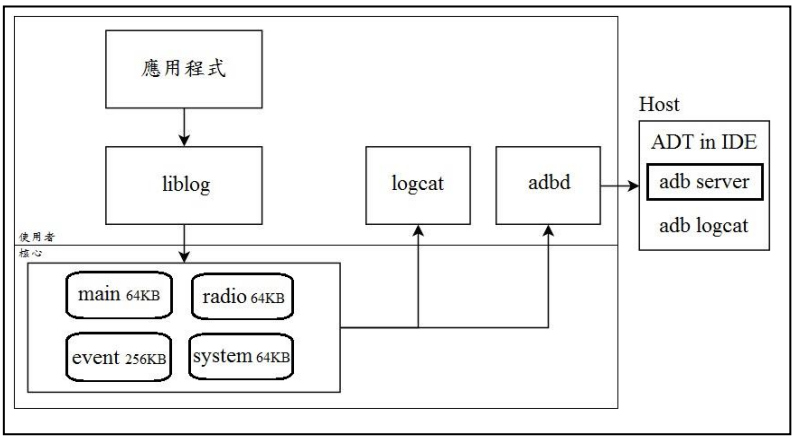

圖 2：Android Log 系統

三、Android 權限框架

為了限制應用程式任意存取敏感的資料，Android 在應用程式框架提供了一個以權限為基礎的安全模型，開發者必須在 AndroidManifest.xml 檔案裡使用<users-permission>標籤來宣告權限的請求，才能獲取相關資料。這些權限總共分為四種保護層級(Faruki et al. 2015)。

（一）一般權限(Normal)

一般權限對於使用者、系統應用程式、裝置本身沒有太大的風險，預設為在安裝時自動被允許。

（二）危險權限(Dangerous)

危險權限因為可以存取隱私資料和使用裝置重要的感測器，所以伴隨著高度的風險，安裝時必須經過使用者同意。

（三）簽章權限(Signature)

如果宣告此類權限的應用程式所使用的開發者憑證與被要求的應用程式相同，在安裝時就會自動被允許。

（四）簽章或系統權限(SignatureOrSystem)

如果宣告這些權限的應用程式使用了和 Android 系統本身或其他被要求的應用程式相同的憑證，在安裝時就會自動被允許。

四、Android Intent

Android 的 Intent 是一個抽象的行為，孫宏明(2013)於書中將其翻譯成中文的意思就是「意圖」，白話一點就是「我想要…」，可以把 Intent 視為是程式和 Android 系統互動的媒介，當程式需要另一個 Activity 或是程式來完成工作時，就可以建立一個 Intent 物件。Intent 同時也是各應用程式之間元件主要的溝通橋樑(Klieber et al. 2014)，通常被大量的使用在開啟不同應用程式之間的活動。

參、系統實作

本章節將介紹本研究的系統開發工具與環境、研究限制、系統架構、系統流程以及詳細說明系統介面與功能規劃。

一、系統開發工具與環境

本研究以跨平台的程式語言 Java 以及 Android 提供的軟體開發套件(Software Development Kit)搭配 Android 系統本身的 Logger 機制進行系統之設計與實作，詳細開發工具與測試環境如表 1 所示。系統呈現的方式為一個可直接運行於 Android 作業系統 5.0 版本以上的應用程式(APK 檔)，可供安裝於行動裝置上進行測試。

表 1：開發工具與測試環境

開發套件	Java SE Development Kit (JDK) 1.8 Android Software Development Kit (SDK) Android Development Tools (ADT)
程式語言	Java
開發環境	Android Studio 1.3 Linux Ubuntu 14.04
測試環境	HTC One E8 Android 5.0.2 LG Nexus 5 Android 5.1.1 ASUS Nexus 7 II Android 6.0

二、研究限制

由於本系統運作環境為 Android 5.0 以上之版本，應用程式對 shell 下 logcat 指令必須搭配 su 指令，才能擁有超級使用者權限(root)。一般來說，搭載 Android 原生系統的 Nexus 系列行動裝置或是其他廠商發表之 Android 行動裝置，並沒有 su 指令可以使用，使用者必須先將裝置的 bootloader 解鎖，才能進行 root 的相關作業。因此本研究將此列為研究限制。

三、系統架構

本研究將各應用程式所宣告之權限擷取出來，從而了解應用程式所擁有的存取權與控制權和可能收集的個人資料。透過 Android API 解析應用程式的 AndroidManifest.xml 檔案，首先，擷取檔案當中使用<users-permission>標籤的片段，列出應用程式宣告的所有權限內容，然後根據 Google 開發者平台公佈的權限介紹以及保護層級的分類(Developer Console 2015)，進而判定應用程式所宣告之權限的安全性及合理性，同時可以瞭解應用程式能夠收集到哪些資料，對於個人隱私造成之衝擊的程度。

然後分析 Android 核心提供的 Logger 紀錄設備所紀錄之活動行為，經由一段程式碼(圖 3)，直接在 shell 裡面對裝置下 logcat 指令，同時使用 grep 指令篩選出應用程式的意圖，以及其他活動紀錄，再根據 Google 開發者平台所公佈之意圖的介紹與使用方式(Developer Console 2015)，分析應用程式的行為。舉例來說，若 Log 紀錄中出現一段字串為"act=android.intent.action.SEND"，代表該應用程式有傳輸資料的行為；若 Log 紀錄中出現一段字串為"act=android.intent.category.APP_BROWSER"，代表該應用程式能夠透過開啟瀏覽器應用程式去瀏覽網路。

```
try
{
   Process p = Runtime.getRuntime( ).exec("su"); //su 指令
   DataOutputStream pp = DataOutputStream(p.getOutputStream( ));
   pp.writeBytes   //logcat 指令，同時使用 grep 篩選關鍵字
      ("logcat –v time –d |grep ' "+pkg+" ' |grep 'android.intent.action.'\n");
   BufferedReader bufferedReader =
      new BufferedReader(new InputStreamReader(p.getInputStream( )));
   pp.writeBytes("exit\n");
   pp.flush( );

   StringBuilder log = new StringBuilder( );
   String line;
   while ((line = bufferedReader.readLine( )) != null)
   {
      log.append(line);
      log.append("\n");
   }
}
```

圖 3：直接在 shell 裡面對裝置下 logcat 指令

最後本研究將各權限以及由 Logger 分析出來的活動，依照其擁有之權限與功能，評估其對於個人隱私造成之衝擊，分成低、中和高三個衝擊程度，然後彙整成風險評估表。表 2 所示為不同權限保護層級對隱私衝擊的程度。不同的意圖對隱私衝擊的程度要視其行為內容決定，以個人資料為基準點，若有傳輸、存取、讀取和寫入資料的行為，將其衝擊程度歸類為高；若有檢視資料的行為，將其衝擊程度歸類為中；若沒有任何使用及接觸資料的行為，可將其衝擊程度歸類為低(表 3)。

表 2：權限衝擊評估表

權限保護層級	衝擊程度	原因說明
一般權限	低	預設允許，但皆無直接存取資料之功能。
危險權限	中	可讀取寫入以及傳輸使用者資料，取得部分系統功能，但需要經過使用者同意。
簽章權限	高	可使用許多系統功能以及連結系統服務，獲得部分管理權限，需要經過簽章認證，但安裝及執行時並未顯示，使用者無法得知該應用程式擁有此權限
簽章或系統權限	高	可使用許多系統功能以及連結系統服務，獲得部分管理權限，需要經過簽章認證，但安裝及執行時並未顯示，使用者無法得知該應用程式擁有此權限

表 3：意圖衝擊評估表

意圖行為	衝擊程度	範例
傳輸、接收、讀取、寫入、修改、複製、刪除資料	高	ACTION_EDIT、ACTION_SEND
檢視、查看資料	中	ACTION_VIEW、ACTION_OPEN_DOCUMENT
無任何使用及接觸資料	低	ACTION_MAIN、ACTION_SHUTDOWN

四、系統流程

本系統參考隱私衝擊評估步驟設計系統流程(圖 4)。

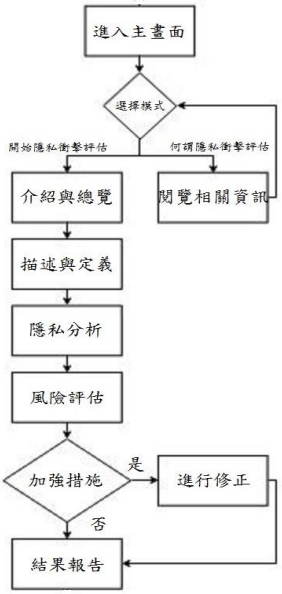

圖 4：系統流程

五、系統介面與功能規劃

系統開始執行會先進入主畫面(圖 5)，可以選擇直接開始隱私衝擊評估或是先閱覽隱私衝擊評估之相關資訊。

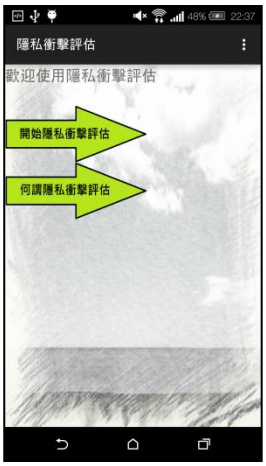

圖 5：應用程式主畫面

若選擇直接開始隱私衝擊評估，系統將進入正式步驟，各步驟之介面與功能規劃詳細說明如下。

（一）介紹與總覽

此介面介紹系統主要的目標和主要的功能，提供使用者閱覽(圖 6)。

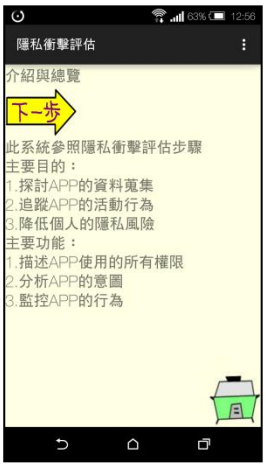

圖 6：介紹主要目標與功能

（二）描述與定義

此介面將列出各應用程式宣告之所有權限。由於透過此方法所擷取出來的權限內容的表示方式為 xml 語法的標籤，因此本系統將 xml 語法的標籤轉換為中文解釋，例如：android.permission.READ_SMS 轉換為「讀取簡訊訊息」；android.permission.ACCESS_FINE_LOCATION 轉換為「存取精確位置」，提供使用者方便閱讀。詳細步驟如下。

1. 列出所有已經安裝於行動裝置內的應用程式(圖 7)。
2. 列出該應用程式實際上宣告的所有權限清單(圖 8)，包含一般權限、危

險權限、簽章權限、簽章或系統權限。

3. Android 權限框架之介紹(圖 9)。

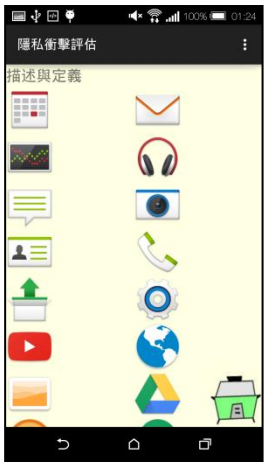

圖 7：列出應用程式

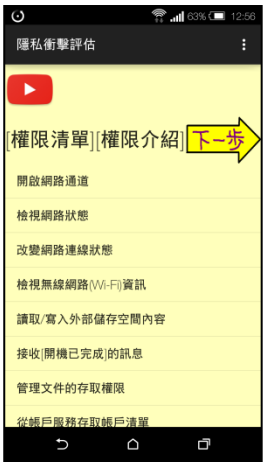

圖 8：列出宣告的權限

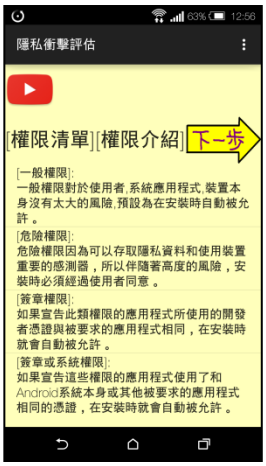

圖 9：權限介紹

（三）隱私分析

此介面將分析 Log 所記錄之活動行為。由於透過此方法收集到的活動紀錄關鍵字為英文 Log 檔，因此本系統將英文 Log 檔轉換為中文解釋，例如：關鍵字為 android.intent.action.VIEW 則轉換為「顯示資料給使用者」；關鍵字為 android.intent.action.SEND 則轉換為「傳遞資料給其他人」，提供使用者方便閱讀。詳細步驟如下。

1. 列出所有已經安裝於行動裝置內的應用程式。
2. 分析 Log，監控應用程式的活動(圖 10；圖 11)。本系統將會顯示日期、時間以及活動的詳細內容。

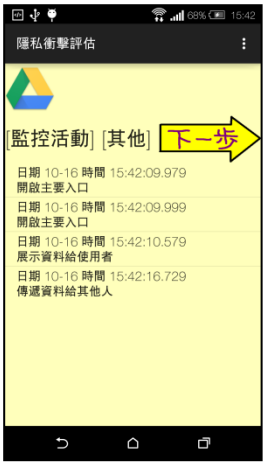

圖 10：監控活動

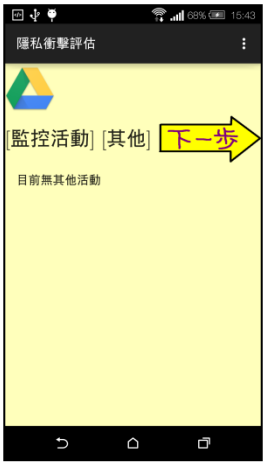

圖 11：其他活動

（四）風險評估

此介面將第二與第三步驟收集之資料匯整成一個風險評估表，表格內容分成五個項目，分別為事件、型態、風險、衝擊程度以及分數，事件為前兩步驟所收集之資料的中文解釋，型態分為權限以及意圖兩種類別，風險為說明事件本身對隱私可能造成之影響，衝擊程度分為低、中和高三種類別，依據本研究之表 2 與表 3 所分類，分數為參考參照國家標準技術研究所之評估尺度

(National Institute of Standards and Technology 2012)，衝擊程度低為 2 分，衝擊程度中為 5 分，衝擊程度高為 8 分，分數越高代表對隱私影響程度越大，反之則越低。本章節以 Google 雲端硬碟應用程式作為範例(表 4)。

表 4：Google 雲端硬碟之風險評估

事件	型態	風險	衝擊程度	分數
開啟主要入口	意圖	應用程式開始執行	低	2
顯示資料給使用者	意圖	使用者可查看資料	中	5
傳輸資料給其他人	意圖	使用者資料被傳輸	高	8
取得照相功能	權限	應用程式擁有執行照相功能的權限	中	5
讀取寫入外部儲存空間內容	權限	應用程式擁有存取外部儲存空間內容的權限	中	5
使用電源管理員的喚醒鎖保持處理器持續	權限	應用程式執行不會因待機而中斷	低	2
開啟網路通道	權限	應用程式擁有開啟網路通道的權限	低	2
檢視網路狀態	權限	應用程式擁有存取網路狀態的權限	低	2
從帳戶服務存取帳戶清單	權限	應用程式擁有存取帳戶清單的權限	低	2
讀取同步設定	權限	應用程式擁有讀取同步設定的權限	低	2
寫入同步設定	權限	應用程式擁有寫入同步設定的權限	低	2
讀取寫入外部儲存空間內容	權限	應用程式擁有存取外部儲存空間內容的權限	中	5
讀取使用者的聯絡人資料	權限	應用程式擁有讀取使用者聯絡人資料的權限	中	5
存取震動	權限	應用程式擁有存取震動的權限	低	2

（五）加強措施

由於隱私衝擊評估的目標是為了解系統對於個人隱私造成的影響，因此本系統並不會強制使用者進行任何加強措施，使用者可以參考第四步驟之風險評估表，依據自己的使用習慣和喜好自行決定是否修正行動裝置的相關設定(圖 12)，或是選擇停止使用該應用程式。若使用者之行動裝置為 Android 6.0 版本以上，可搭配應用程式之權限管理的設定頁面(圖 13)，將不需要之功能關閉，以達到更佳的隱私保護。

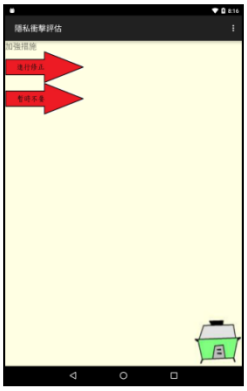

圖 12：是否修正

圖 13：權限管理設定頁面

（六）結果報告

隱私衝擊評估之結果因人而異，各個行動裝置不同的設定、不同的應用程式甚至不同廠牌之測試結果不盡相同，此介面將顯示風險評估結果之評估分數，例如：Google 雲端硬碟之評估分數為 3.5 分。然後再將所有安裝於行動裝置上的應用程式之測試結果的評估分數加總起來，依照系統評估分數公式（系統隱私衝擊評估分數 $=\frac{\text{所有應用程式之評估分數總和}}{\text{行動裝置應用程式之總共數量}}$）得出最後的隱私衝擊評估分數。

肆、系統測試結果與發現

本研究於系統測試時發現，隱私衝擊評估第二步驟(描述與定義)所列出之權限清單與 Google Play 商店下載時所顯示的權限要求並非一模一樣，也就是說，一般於商店下載或是自行從第三方安裝之應用程式，僅僅顯示「危險權限」給使用者，其餘三種類型之權限就算宣告於 AndroidManifest.xml 檔案裡，使用者也無法從表面得知。雖然一般權限皆無直接存取資料之功能，簽章、簽章或系統權限也都需要通過簽章認證才能使用，但以使用者的立場思考，Android 在此方面應該提供給客戶更詳細的資訊。

伍、結論

本系統提供一個友善且中文化的使用介面，透過分析應用程式宣告之權限以及系統之 Log 紀錄，搭配隱私衝擊評估明確的步驟，讓使用者清楚了解行動裝置對於個人隱私的影響。由於本系統實作方式為一個可直接運行於 Android 作業系統 5.0 版本以上的應用程式，不需要透過網路連線伺服器端或是使用傳輸線連結其他電腦，即可進行完整的隱私衝擊評估，為使用者帶來便利的攜帶性，同時可以減少網路連線或是連結其他電腦可能帶來的隱私風險，降低使用者對於本系統的疑慮。然而，本研究之研究限制有關於 Android 本身沒有 su 指令可以使用，要取得超級使用者權限才能進行的部分，未來將繼續探討此問題，期望能夠在安全為前提之情況於技術上突破 Android 此一限制。

陸、參考文獻

1. 孫宏明，2013，Android 4.X 手機/平板電腦程式設計入門、應用到精通，臺北：碁峰資訊。
2. Drake, J. J., Fora, P. O., Lanier, Z., Mulliner, C., Ridley, S. A., Wicherski, G. *Android Hacker's Handbook*, Wiley, 2014.
3. Developer Console. "Intent" October 2015 (available online at http://developer.android.com/intl/zh-tw/reference/android/content/Intent.html).
4. Developer Console. "Manifest.permission" October 2015 (available online at http://developer.android.com/intl/zh-tw/reference/android/Manifest.permission.html).
5. Faruki, P., Bharmal, A., Laxmi, V., Ganmoor, V., Gaur, M. S., Conti, M., and Rajarajan,

M. 2015. "Android Security: A Survey of Issues, Malware Penetration and Defenses" Communications Surveys & Tutorials, IEEE (17:2).

6. Gartner. "Gartner Says Smartphone Sales Surpassed One Billion Units in 2014" March 2015 (available online at http://www.gartner.com/newsroom/id/2996817).
7. International Data Corporation. "Smartphone OS Market Share, 2015 Q2" August 2015 (available online at http://www.idc.com/prodserv/smartphone-os-market-share.jsp).
8. Information Commissioner's Office. 2014. " Conducting privacy impact assessments code of practice ", pp 3-5.
9. Klieber, W., Flynn, L., Bhosale, A., Jia, L., and Bauer, L. 2014. "Android Taint Flow Analysis for App Sets" ACM SIGPLAN International Workshop on the State of the Art in Java Program Analysis.
10. Ministry of Technology, Innovation and Citizens'Services. 2014. "Ministry Privacy Impact Assessment Guidelines", pp 2-11
11. National Institute of Standards and Technology. 2015. "SECURING ELECTRONIC HEALTH RECORDS ON MOBILE DEVICES", pp 23-34.
12. National Institute of Standards and Technology. 2012. "Guide for Conducting Risk Assessments", pp 67-68.
13. Office of the Privacy Commissioner. 2007. " Privacy Impact Assessment Handbook ", pp 5, pp 21-27.
14. Yaghmour, K. *Embedded Android*, O'Reilly Media, 2013.