Android 使用安全設計之探討

何煒華
東吳大學資訊管理系
副教授
e-mail：
whhe@csim.scu.edu.tw

謝長軒
東吳大學資訊管理系
研究生
e-mail：
changhsuan@gmail.com

摘要

行動裝置除了提供通訊功能外，還能提供多元功能，因此包含了更多的敏感性資訊。本論文對 Android 手機的安全控制措施進行分類，並提出建議的安全設定。提供使用者在使用手機時能確認相關的安全設定，以確保使用的資訊安全認知，並降低資安事件的產生。

關鍵詞：行動裝置、Android、資訊安全認知

Abstract

Except the daily communication function, mobile devices provide variety of functions. Therefore, they contain more sensitive information. In this paper, security controls are categorized and security settings are recommended for Android phones. This provides users to confirm the relevant security settings when using Android phones. Information security awareness can be assured, and information security events will be reduced.

Keywords: mobile device, Android, security awareness

1. 前言

行動裝置的普及率愈來愈高，透過行動裝置上網的使用率也僅次於使用電腦的數量[2]。當行動裝置有更多應用及與外面連結傳輸及儲存資料的同時也代表面對更多的資安威脅。但行動裝置的使用者遍佈的族群更廣泛，是否這些使用者都有意識到使用行動裝置的同時，也在面對這些潛在的威脅。

1.1 研究背景與動機

在台灣現在的主流手機平台主要為 Apple iOS 及 Google Android。相較與 Apple iOS 封閉式的平台，Android 為開放式平台，從 2009 年開始在行動裝置的市佔率以驚人幅度成長，到 2013 年的統計資料已顯示有超過 70%的行動裝置作業系統為 Android。根據趨勢科技調查，有 76.8% 的國人使用桌上型電腦上網，其後依序為 Android 手機（72.5%）、筆記型電腦（50.2%）、平板電腦（32.3%）、iPhone（15.4%）以及 Mac 電腦（3.1%）[2]。而又以 Android 4.4 代號 Kitkat 的版本市佔率（39.1%）最高[4]。

Version	Codename	API	Distribution
2.2	Froyo	8	0.2%
2.3.3 - 2.3.7	Gingerbread	10	3.0%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	2.7%
4.1.x	Jelly Bean	16	9.0%
4.2.x		17	12.2%
4.3		18	3.5%
4.4	KitKat	19	36.1%
5.0	Lollipop	21	16.9%
5.1		22	15.7%
6.0	Marshmallow	23	0.7%

Data collected during a 7-day period ending on January 4, 2016.
Any versions with less than 0.1% distribution are not shown.

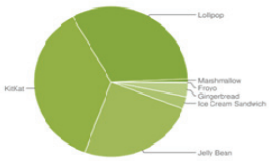

圖 1 Android 各版本市佔率分配
參考來源：Android Platform Versions [4]

因為現在的手機功能愈來愈多元化，除了打電話，傳簡訊及傳送 email 外，透過手機作業系統平台及手機應用程式的應用，整合了更多不同的運用。包含提供電子交易的服務，娛樂性的應用，各種照片及多媒體資料的存取應用及整合雲端的各種服務，可讓使用者更方便透過行動裝置就能存取、同步及使用各種不同的資訊服務。讓手機成為了愈來愈重要的行動裝置[2]。因此儲存在手機行動裝置中的敏感性資料也愈來愈多了。使用者除了在意手機的隱私問題外，也開始擔心這些敏感性資料是否會被其他使用者所存取及使用[9]。包含透過手機進行電子銀行的轉帳交易，各種生活上使用的資料儲存在手機中方便使用，這些資訊都有可能因為手機使用時的不慎造成資訊外洩成為新的資安事件。

隨著手機應用功能的增加，資安風險的相關事件也逐年成長。從 2010 年，發現第一隻 Android 的惡意程式開始[5]。行動裝置所需要的資訊安全防護開始受到重視。開始有許多研究專注於手機手機應用程式的安全機制、Android 作業系統安全機制…等的比較。如同過往我們在電腦上所要求的一樣，也需要透過適當的機制來保護行動裝置資料的安全性

[1][17]。

為了預防現在的各種資安威脅，使用者需要更多的資安保護措施[4][5]。一部分資安防護功能可透過行動裝置本身內建提供的。譬如：Android 各種功能存取權限及資料加密功能等。另一部分則需要透過額外附加的控制措施來降低資訊安全事件所造成危害的風險。譬如：安裝防毒軟體及對資訊安全認知的教育訓練等[9]。只有互相搭配使用，才能有效的降低資訊安全事件發生的機率降低風險[5]。

1.2 研究目的

在已往的研究中，主要是針對手機平台的安全性或是手機 App 的安全機制來做研究，較少著重在使用者對安全認知的相關研究。直到最近開始有相關調查使用者對手機平台使用時，最在意的是個人隱私資料是否會被第三方未經授權的使用者取得[3]。但同時也有研究發現，一般使用者對於資訊安全相關知識是較為不足的。

2. 相關文獻探討

2.1 Android 行動作業系統

Android 是一個以 Linux 為基礎的開放原始碼行動裝置作業系統，主要用於智慧型手機、平版電腦等行動裝置的作業系統，由 Google 成立的 Open Handset Alliance (OHA，開放手持裝置聯盟) 持續領導與開發中。Android 已發佈的最新版本為 Android 6.0 (Marshmallow) ，但現在手機裝置市佔率最高仍為 4.4 約 36.1%，次高的為 Android 5.0 (Lollipop) [16]。

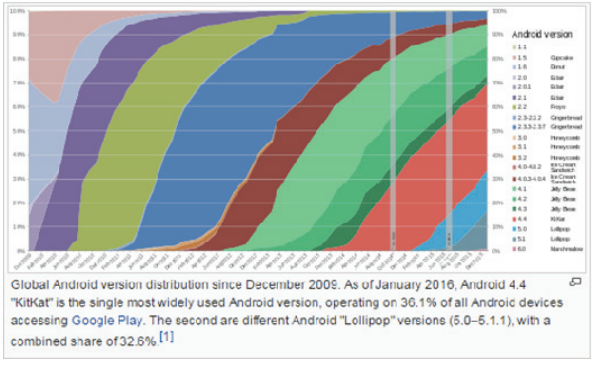

圖 2 Android 各版本市佔率分配
參考來源：Android Version History[16]

2.2 Android 應用程式發佈流程的差異所造成的安全性風險

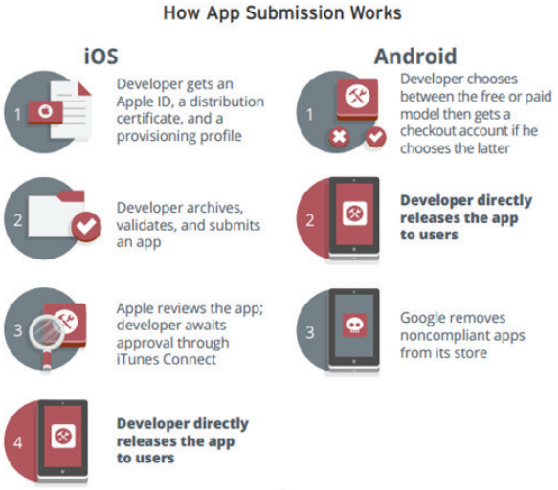

圖 3 iOS 及 Android 應用程式發佈的差異
參考來源：TrendLabs 2013 Annual Security Roundup [13]

Android 手機應用程式開發過程中，與 iOS 不同的地方是，iOS 需要經過 Apple 去檢視後才能出版。Android 的開發者，只需開發者自行確認後，Google 只會檢查手機/平版的版本相容性，並不會針對程式內容做檢查就可直接出版。若 Android 手機應用程式中包含惡意程式或是對手機上資料進行相關存取，只能依賴使用者在下載及使用手機應用程式時，確認手機應用程式的來源及所需權限的來降低資安風險。

2.3 Android 手機相關權限設定資訊

在每個 Android 手機應用程式安裝時，會顯示該應用程式所需要使用的權限資訊。需使用者接受後，才會開始下載安裝。主要幾種常見會顯示的權限資訊包含：

位置資訊權限：分為兩種型式：一種為概略地點，只使用 Wi-Fi 及行動網路基地台進行定位服務。另一種為精確地點，會使用 GPS 及其他網路資訊協助定位。位置資訊就跟使用社群軟體一樣，讓應用程式搜集使用手機應用程式時所在的地點資訊。

裝置狀態及識別碼相關權限：允許這個權限，可以讓 Apps 讀取裝置上包含來電資訊及手機的國際移動設備識別碼 (International Mobile Equipment Identity, IMEI) 可用來辨識每一部手機的識別碼，就像是手機身份證一樣。當要允許此權限時，需先確認該手機應用程式是否需要讀取手機的狀態資訊，再決定是否需要允許。

讀取您的通訊錄和修改您的連絡人：修改

連絡人權限，可以讓手機應用程式存取並修改相關聯絡人資訊。讀取您的通訊錄權限，可以讓手機應用程式讀取全部的通訊錄資料，並包含最常聯絡人的相關資訊。除了手機撥號、簡訊服務的手機應用程式外，其他手機應用程式要使用這些權限時，建議確認是否需要允許及是否有其需要。

文字訊息相關權限：如果惡意程式擁有此權限後，透過亂發訊息可能會讓人電話費暴增。另外讀取您的文字訊息及接收文字訊息，可能會讓您的隱私資料曝光。所以當要允許手機應用程式取得此權限時，最好能了解使用的原因再允許使用。

帳號相關的權限：“尋找此裝置的帳號”，此權限讓手機應用程式可以存取帳號管理員並取得這隻手機上所有相關手機應用程式使用的帳號資訊。”使用此裝置的帳號”，讓手機應用程式可以存取此裝置，不會再跳任何權限需求資訊。”建立帳號及設定密碼”， 可以讓手機應用程式讀取帳號的相關驗證訊息。因此若是有惡意程式使用此權限，可以持續使用您的帳號做任何事情。因此在安全性的考慮上需要確認使用的原因再允許使用。

在每個 Android 手機的「設定」中「安全性」裡，可以檢示手機安全性的相關設定。譬如：不明來源。預設沒勾選的狀態下，只能安裝從 Google Play 提供的應用程式。勾選後，就能允許各種來源來的手機應用程式程式都可安裝。但除非完全瞭解該動作的風險，一般不建議修改此項設定。

除了可透過 Android 手機的安全性確認應用程式的安裝來源外，使用者若想瞭解手機中安裝了那些應用程式及這些應用程式使用了那些權限。則可透過手機中的可透過手機中的「設定」中「應用程式」來查看該應用程式被授與了那些權限。

3. Android 行動裝置資訊安全認知文獻探討

3.1 Android 手機資安事件統計

到 2014 年 3 月，Android 平台上惡意程式已經超過 2 百萬個[12]。而且成長的速度還在增加。另從研究報告中，指出最常出現的幾種權限應用錯誤造成的資安事件。

Network-based/GPS Location：透過手機定位或是 Wi-Fi 取得定位資訊。可以讓開發者提供區域化的廣告，但也可讓攻擊者提供特定區域或語言的惡意程式。

圖 4 Android 應用程式含有惡意程式統計圖
參考來源：趨勢科技新聞[12]

檢視網路狀態：允許應用程式檢視網路資訊，包含 3/4G 連線資訊及 Wi-Fi 連線資訊，用來提供更新資訊或是連線到特定網站。但也可能會被惡意程式利用，偷偷建立持續的連線，導致電力使用及網路流量使用超過預期。增加額外的成本或不便。

檢視 Wi-Fi 狀態：可讓手機應用程式存取 Wi-Fi 資訊。但也可被利用知道 Wi-Fi 的資訊，透過已知的漏洞進行攻擊或是偷取 Wi-Fi 密碼。

取得正在執行應用程式清單：可讓手機應用程式辨識那些程序在執行。亦可被利用取得程序清單後，將特定程度刪除。通常是將保護手機機制的應用程式做程序停用。譬如：將防毒軟體防護程序停用。

允許存取網際網路：讓應用程式可以存取網際網路。惡意程式可透用此權限在使用者不知道的狀況，連上網路下載其他惡意程式。或是對特定主機進行遠端攻擊。

讀取手機狀態及辨識資訊：可讓手機應用程式讀取手機辨識碼或相關手機資訊。有些程式只會檢視手機資訊來做辨識的動作，擁有此權限就可假冒成該手機進行相關存取。

開機自動啟動權限：讓後應用程式在開機後自動執行的權限。惡意程式取得此權限後，將會在每次開機後就自動執行，監控整個手機開機後的所有活動行為。

控制振動通知權限：此權限可停止正常系統告警的振動機制。讓使用者更不容易知道手機的異常行為狀態。

睡眠機制權限：控制是否會進入睡眠待機模式。惡意程式擁有此權限，就可確保惡意程式即使在看似休眠中的狀態持續進行檔案的傳輸。

讀取/刪除 SD Card 資料:讓手機應用程式可以讀取外接儲存空間。擁有此權限時，可以

將 SD card 上的資料傳送到其他網站，或是將 SD card 上儲存的資料刪除。

傳送簡訊：允許手機應用程式傳送簡訊資料。擁有此權限的惡意程式，可以傳送簡訊，造成大量額外的費用。或是利用此途徑將敏感性資訊送出。

上述為幾種常見的 Android 權限可能造成的風險事件。隨著應用程式的種類多元化，所需的權限也大不相同。所以在允許使用時，需要更加注意[18][22]。

3.2 行動裝置常見的惡意程式及分類

防毒軟體公司趨勢科技也公布十大惡意程式排行，包含：偽應用程式 30% 、資料竊取軟體 (21%) 、廣告軟體 (18%) 、高價服務濫用 (14%) 、遠端控制木馬程式 Rooter/RAT (13%) 和惡意下載軟體 (4%) [2][3]。依常見的惡意程式並依惡意程式的行為類型可簡易分類[6] [8]如下：

銷售/竊取使用者個人資訊：透過手機安裝的應用程式取得使用者的相關訊息，包含：使用者位置、通訊錄清單及手機的 IMEI 碼等。大部份的惡意程式取得這些資訊是為了能夠取得使用者的財務相關資訊如銀行帳號及密碼等。

盜打電話或傳送訊息：此惡意程式會偷偷送出簡訊或撥打高額付費電話[10]。傳送簡訊可以讓該手機變成寄送廣告簡訊的平台，而且不易追蹤到真正廣告簡訊的發起端來源。甚至有些惡意程式更利用簡訊的方式送出遠端指令進行搖控攻擊的行為[22]。除了會被誤當為廣告簡訊來源或是惡意攻擊來源之外，還會需要付擔額外的電信費用。

惡意廣告軟體行為：惡意程式透過安裝在手機上時，依據取得使用者上網的記錄資訊，增加特定目標的網頁點擊率，優化該網站在搜尋引擎中的排名。此種行為除了會增加使用者網路使用率及手機電量的使用外，還會洩露使用者上網的習慣隱私訊息[20]。有的甚至跟電腦的廣告軟體一樣，在使用手機應用程式時，自動跳出廣告訊息或是惡意訊息，讓使用者誤觸造成進一步的攻擊型為，如：對特定目標進行分散式阻斷攻擊 (Distributed Denial of Service,由多台裝置對單一特定服務進行大量存取造成該目標無法正常提供服務) [18]。

竊取信用卡或手機支付相關訊息：NFC (Near Field Communication) 已可應用在 Android 手機上進行近距離交易，但也增加了安全性的風險。惡意程式，可以借此竊取交易的信用卡相關資訊[21]。

針對這些惡程式的行為有研究發現，大部份的惡意程式都是透過使用者因在安裝手機應用程式時同意給予了錯誤的權限限制，導致這些應用程式可以進行相對應的行為。因此在安裝任何手機應用程式前務必確認相關的使用權限資訊。

3.3 行動裝置常見的安全性威脅

現在手機功能愈來愈強大，使用者對手機的依賴性也愈來愈高。除了手機相關的安全設定外，包含手機資料的保護及手機遺失時的相關處理都需要特別的注意，已避免當手機遺失時，相關的資料包含電子郵件、照片及個人隱私都跟著曝光洩露，造成更嚴重的損失。常見的安全性威脅及說明如下[25]：

使用手機連到惡意網站造成資料外洩：現在手機的功能相關方便，不在只是收發簡訊及撥打電話。也能連上網際網路，連接社群應用。若是使用者一不注意，誤點到釣魚訊息或是瀏覽到惡意網站，都有可能造成自身帳戶密碼的資訊外洩或是將手機上的敏感性資料分享至公開網路上，造成進一步的資安事件。

使用不安全的網路連線：利用手機使用免費的公用 Wi-Fi 網路，剛好有心人事或駭客可輕鬆側錄到相關傳送資料。造成敏感性資料外洩，如：身份證字號、信用卡號碼等。

安裝不安全的應用程式：手機上誤裝惡意的應用程式或是對安裝手機應用程式的權限認知不足。導致有心人士透過惡意程式的功能將手機上的敏感性資料公開上傳，造成資安事件的產生[9]。

手機遺失造成資料的遺失：除了手機的操作不慎造成的資安事件外，手機的遺失也是常見的威脅。北美知名電信商研究報告指出每日超過 20 萬的手機遺失或是損害，造成手機使用者的不便[15]。若是手機沒有設定足夠的安全設定及對手機上資料做加密的處理，當手機遺失時，撿到手機的人就可以輕易查看裡面的資訊。若手機資料未有效備份處理，當手機遺失或故障時，裡面的資料也無法在存取一樣會造成難以估計的損失。

3.4 行動裝置的安全設定建議

基於前述所提的相關安全性威脅，各資訊安全廠商及研究安全機構針對 Android 手機所提供的安全設定提出相關建議的設定及注意事項[11]。用來避免及降低資安風險及事件的

產生。以下是整理資安廠商所提供的基本手機安全設定建議：

不在手機上自動儲存密碼：許多人在瀏覽網頁或應用程式時會自動記錄密碼，雖然可以方便使用者使用。但也方便當有人借用手機時，也能輕易就能瞭解及登入該網站或應用程式並存取相關資訊。不在手機上自動儲存密碼，可避免當別人使用此手機裝置時，多一道保障避免陌生人登入或存取相關資訊。

使用手機內建的安全設定：手機通常會提供一些基本的安全性選項。譬如：螢幕鎖定、資料加密功能。啟用這些功能，可以增加當有人取得手機時，登入手機的困難性。另外建議設定手機密碼時，不要使用太過簡單易猜的密碼，這樣就失去設定密碼的意義了。

將手機應用程式鎖定：將有使用敏感性資料的手機應用程式上鎖。可利用第三方的手機應用程式程式，當使用者要開啟這些含有敏感性應用程式時，需要額外輸入驗證機制。這樣即使有借用手機或手機遺失時，不致於可存取上面安裝的手機應用程式。此建議設定，不需套用在所有的手機應用程式上，只需要套用在含有敏感性資料上的手機應用程式即可[14]。

瞭解手機應用程式使用權限的重要性：當在安裝手機應用程式時，Android 手機會提示該手機應用程式會使用那些相關權限。瞭解該手機應用程式會使用那些權限是很重要的一件事。可以讓使用者知道此手機應用程式可以存取到那些資料[24]。若是無法瞭解權限裡的內容，至少可參考一下有相關安裝該手機應用程式的使用反饋資訊或是評比分數，來做為使用該手機應用程式前的基本參考。另外就是不要從不信任的來源下載相關手機應用程式[7] [14] [23]。

使用安全的網路：當在公用場合使用公開免費的 Wi-Fi 時，容易讓旁邊的有心人士借此監聽您的網路傳輸資料，若傳輸資料未加密時，將會造成資訊外洩。若此時還有傳輸安全性或敏感性資料時，將會造成資訊外漏[14]。

使用安全性軟體應用程式保護行動裝置：建議在手機上安裝防毒軟體，可針對惡意程式偵測監控外，也對手機瀏覽網頁時提供多一份安全的防護。

建立手機備份資料：此為建議必要選項。當手機被偷或故障造成裡面的資料無法存取時，還可透過定期備份手機資料的方式。將遺失的資料還原。若是手機遺失，最佳的處理方式是將手機的資料全部清除，此時若有備份資料就可以不用擔心是否會因為移除資料造成資料無法還原的損失。

啟用手機追蹤功能：當手機遺失或被偷還想把手機找回。那至少先有在手機上開啟此功能。這樣當手機遺失時，還有機會透過 GPS 定位的方式找到手機最後出現的地點進行搜尋。若未開啟此功能，那連最後找回手機的機會都沒了。

啟用遠端清除手機資料功能：此功能是當手機遺失或被偷竊時，可透過遠端控制的方式將手機的資料完整的清除，避免手機裡的資料外洩。

4. Android 手機的安全控制分類整理與防護目的

4.1 基本手機安全設定

設定 SIM 卡鎖：此功能是當手機開機時必需先輸入 SIM 卡密碼正確才能進入開機程序。設定此功能，除了因為要啟用資料加密時需要設定外，還可避免當有人撿到該手機，將該 SIM 卡取出後，直接開機開始使用。建議設定此項目。設定方式：至手機「設定」中「安全性」選項裡「設定 SIM 卡鎖」。

設定螢幕鎖定功能：設定此功能後，使用該手機的人必需先解鎖後才能開始使用，可避免陌生人撿拾手機後直接使用。建議所有使用者必需設定此項目設定，並且設定為 PIN 碼，除了可增加陌生人使用手機解鎖困難外，並在設定資料加密時，會利用此碼將手機相關資料做加密動作。設定方式：至手機「設定」中「安全性」選項裡「螢幕鎖定」選擇「PIN 碼」並輸入 PIN 碼。

設定螢幕自動鎖定功能：此功能是當手機未使用時，經過設定時間後，自動上鎖。可避免使用者使用手機後未將手機上鎖，造成旁人拿取手機時可直接讀取該手機資訊或直接使用手機功能。建議設定此項目功能。設定方式：至手機「設定」中「安全性」選項裡點選「自動鎖定」，並設定經過多久就自動將螢幕鎖定。

手機資料加密功能項目：此功能能將手機存取的資料加密包含記憶卡資料一起加密。可避免當有人拾獲手機時，將記憶卡取出直接讀取裡面相關資訊。建議啟用該設定，來避免當人拾獲手機時能輕易讀取裡面相關資料。設定前先確認有啟用設定螢幕鎖定。設定方式：至手機「設定」中「安全性」選項裡點選「對手機進行加密」。設定完成後需要重新啟用手

機，並在每次重新啟動手機時都需輸入 PIN 碼後才會開機。

4.2 手機網路相關安全設定

關閉 Wi-Fi 無線網路設定：此功能是將手機無線網路功能關閉。建議是不使用無線網路可以關閉。當開啟使用時也需注意。若是在公用無線網路場合避免使用未加密的無線網路服務。除了可避免在公開環境被人側錄網路傳輸資料外，也可避免登入到假的無線網路服務，被盜取相關隱私資訊。設定方式：至手機「設定」中「無線與網路」選項裡的「Wi-Fi」調整成「關閉」。

關閉藍芽設定：此功能是將藍芽網路設定關閉。建議是不使用時就將此功能關閉。啟用時，也需注意配對設備是否為確認可連結的設備再輸入所需驗証碼。這樣可以避免與未知的設備做連結而誤傳手機中的相關資訊。設定方式：至手機「設定」中「無線與網路」選項裡的「藍芽」調整成「關閉」

關閉可攜式無線基台設定：關閉可攜式無線基地台，除了可以節省手機電池的使用外。更重要的是可避免因開放無線基地台功能給別人連接使用時，未經授權的設備也一起使用了該分享連線。除了會佔用頻寬外，更可能讓未經授權的設備竊聽網路傳輸的資訊或是遭守對方遠端連線的攻擊。建議是關閉此設定，除了在必要使用的環境下才開啟使用。而且開啟使用時，要連線的設備必須輸入正確的驗証密碼後才能使用。設定方式：至手機「設定」中「無線與網路」點選「更多」在裡面的「數據連線與可攜式無線基地台」勾選「可攜式 Wi-Fi 無線基地台」來啟用設定。接著點選「可攜式 Wi-Fi 無線基地台設定」中「配置 Wi-Fi 無線基地台」將「安全性」設定改為「WPA2-PSK」並輸入密碼。只後需要連接此無線訊號的裝置必需知道密碼後才可連線。

使用行動網路：此功能預設是開啟的，使用此功能時手機會利用行動網路業者提供的網路服務讓使用者進行上網的功能。建議是開啟的，因為包含手機遺失等定位及搜尋功能都會用到此服務，但若是到國外使用時，建議先確認網路費率後才開啟。已避免網路費用爆增。設定方式：至手機「設定」中的「無線與網路」點選「更多」選項裡的「行動網路」並勾選啟用「行動數據連線傳輸」。有勾選此項目，手機才會透過電信業者提供的行動網路進行資料傳輸。

關閉無線及 GPS 定位設定：關閉此設定可避免手機應用程式利用無線網路或行動網路，搜集使用者手機裝置的位置，進而分析使用者習慣出沒的地方。建議當有使用需求時再開啟該設定。如使用地圖導航功能時。設定方式：至手機「設定」中「位置」選項裡，將「模式」更改為僅限裝置 GPS。

關閉定位行動資料傳輸：此功能與上述功能不同是，上述功能是允不允許手機提供定位資訊。此功能為是否要將定位的資料傳送至 Google 定位記錄。此服務是可以讓使用者去追蹤該手機有去過那些地方。建議是關閉此服務。避免第三方單位利用搜集使用者定位記錄，分析使用者習慣及出沒的地方。設定方式：至手機「設定」中「位置」選項裡的「定位服務」點選「Google 定位紀錄」調整成「關閉啟用」。

4.3 手機應用程式相關設定

在 Android 手機中，此類型相關設定雖然不多，但最為重要。也最容易被使用者忽視的設定項目。

設定手機應用程式安裝來源：強烈建議不要從非信任的來源下載應用程式。一旦允許從不明來源安裝應用程式時，任何惡意程式都有機會透過此功能將木馬或是其他惡意程式下載至手機中。建議是絕對不要勾選啟用允許從不明來源安裝應用程式。設定確認方式：至手機「設定」中「安全性」選項裡，確認未勾取「不明來源」項目。

確認各手機應用程式使用權限：此功能主要的目的是讓使用者知道，手機裡面有安裝了那些應用程式並且知道這些應用程式可以存取那些權限。在前面提到的各種因為權限的關係所造成的風險或是威脅，百分之九十都是因為應用程式的權限所造成的。所以知道如何查看該應用程式有那些權限對使用 Android 手機的使用者來說是非常重要的。如果查看的方式：至手機「設定」中「應用程式清單」裡，點選要查看的每個應用程式名稱並檢視權限內容。

保持應用程式的更新：因為手機應用程式就跟電腦作業系統一樣，可能使用久了發現有些安全性的漏洞就必需透過應用程式更新來修復這些漏洞避免造成進一步的災害。設定方式：至手機點選「Play 商店」，可從目錄項目中點選「我的應用程式」，並針對需要更新的應用程式點選「更新」進行更新即可。

4.4 手機資料相關設定

手機資料相關設定主要是針對手機裡的資料備份及當手機遺失時如何處理做說明介紹。尤其是手機遺失後的處理，一定要記得進行相關資料清除動作，才能避免進一步的風險。

手機備份設定：此功能是將手機裡存放的資料，進行資料備份。未來當手機遺失及故障時可以將資料還原使用。Android 手機已經有與 Google 帳號作連結。當手機遺失或故障後，可在新手機上套用相同的帳號，即可將原有手機的資料透過帳號的連結將資料還原。設定方式：至手機「設定」中「備份與重設」選項裡，勾選「備份我的資料」並設定備份帳號。待同步後，就會將手機裡的相關資料備份一份在設定的備份帳號中。之後手機只要透過此帳號，就可以進行還原。

手機遺失設定—清除手機資料：此功能會將手機上的資料清除並還原成手機出廠預設值。當確認手機遺失後，請進行相關步驟，已避免手機裡的訊息、照片及其他相關資訊外洩。執行方式：登入網頁 Google Android 裝置管理員點選清除。一旦點選後，當手機連上線，就會自動進行還原預設值的動作，將手機裡的資料清除。此步驟是最後的手段，可避免手機遺失後讓人輕易的取得手機裡的重要資料。

上述為 Android 手機的相關安全性功能介紹及說明，主要是針對常見的威脅做預防及事後補救的動作。希望能讓使用者瞭解到手機廠商針對常見的手機威脅是有提供基本的對應方式，但除了依靠手機廠商外，還是需要使用者在資訊安全的認知上有所提昇才能有效降低資安事件的風險。

5. 結論與未來展望

本論文透過了解 Android 手機所提供的基本安全控制措施依照性質進行分類整理，並提出建議的基本安全設定。提供使用者在使用手機時能確認相關的安全設定，以確保使用的資訊安全認知，並降低資安事件的產生。

展望未來研究可進一步透過問卷調查的方式，將分類項目結合問卷題項，評估 Android 手機使用者對使用 Android 手機時的安全認知及手機的資訊安全問題是否有所注意。瞭解未來是否需要加強使用習慣的相關教育訓練來強化對使用手機的安全認知，以更有效的預防資安事件的產生。

參考文獻

[1] 行政院研究發展考核委員會。***101 年度行動裝置資安防護參考指引***, 2012。

[2] 趨勢科技。趨勢科技：台 Android 手機上網普及率僅次於桌機。民 103 年 10 月，取自 http://technews.tw/2014/10/06/tw-popularity-of-network-android-user/

[3] 趨勢科技。趨勢科技新聞：資料安全威脅是行動世代的最大隱憂針對 Android 行動惡意程式數量持續飆升 擁抱 BYOD 資安防護不可少。民 101 年，取自 http://www.trendmicro.tw/tw/about-us/newsroom/releases/articles/20121030014735.html

[4] Android. Android Platform Versions. (2016, January 4). Retrieved from https://developer.android.com/about/dashboards/index.html

[5] Cnet. Android gets its first texting malware. (2010, August 11). Retrieved from http://www.cnet.com/news/android-gets-its-first-texting-malware/

[6] G Data Software AG. G DATA MOBILE MALWARE REPORT THREAT REPORT:Q2/2015. (2015, July). Retrieved from https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/G_DATA_MobileMWR_Q2_2015_US.pdf

[7] Hongkiat. 10 Tips To Tighten Security On Your Android Device. Retrieved from http://www.hongkiat.com/blog/protect-your-android-device/

[8] IBM. Mobile Malware Threats in 2015: Fraudsters Are Still Two Steps Ahead. (2015, July 13). Retrieved from https://securityintelligence.com/mobile-malware-threats-in-2015-fraudsters-are-still-two-steps-ahead/

[9] Symantec. Android.geinimi. (2011, January). Retrieved from http://www.symantec.com/security_response/writeup.jsp?docid=2011-010111-5403-99

[10] Techradar. Expensive virus hits Android users. (2010, August). Retrieved from http://www.techradar.com/news/phone-and-communications/mobile-phones/expensive-virus-hits-android-users-709260

[11] Trend Micro. 7 Android Security Hacks You Need to Do Right Now. (2015, June 10). Retrieved from http://www.trendmicro.com/vinfo/us/security/news/mobile-safety/7-android-security-hacks-you-need-to-do-right-now

[12] Trend Micro. Mobile Malware and High Risk Apps Reach 2M Mark, Go for "Firsts". (2014, March 26). Retrieved from http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-malware-and-high-risk-apps-reach-2m-mark-go-for-firsts/

[13] Trend Micro. Trend Labs 2013 Annual Security Roundup. (2014, January 14). Retrieved from http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-cashing-in-on-digital-information.pdf

[14] Verizon. 8 common-sense tips to keep your smartphone secure. (nd). Retrieved from http://www.verizonwireless.com/mobile-living/network-and-plans/security-app-tips-to-keep-your-smartphone-secure/

[15] Verizon. Smart phone thefts rose to 3.1 million in 2013. (2014, May 28). Retrieved from http://www.verizonwireless.com/mobile-living/network-and-plans/security-app-tips-to-keep-your-smartphone-secure/

[16] Weikipedia. Android Version History. (2016, January). Retrieved from http://en.wikipedia.org/wiki/Android_version_history

[17] Androulidakis, I., & Kandus, G.. Mobile Phone Security Awareness and Practices of Students. ***The Sixth International Conference on Digital Telecommunications***, pp. 18-24, 2011.

[18] Felt, A. P., Finifter M., Chin, E., Hanna, S., and Wagner, D. A Survey of Mobile Malware in The Wild. ***Security and Privacy in Smartphones***, 2011.

[19] Furnell, S. M., Bryant, P., & Phippen, A. D. Assessing the security perceptions of personal Internet users. ***Computers & Security***, Vol 26, No. 5, pp.410-417, 2007.

[20] National Institute of Standards and Technology, ***Security and Privacy Controls for Federal Information Systems and Organizations***, American, Author, 2013.

[21] Mulliner, C. Vulnerability Analysis and Attacks on NFC-enabled Mobile Phones. Paper presented at ***the 1st International Workshop on Sensor Security (IWSS)*** at ARES, Fukuoka, Japan, 2009.

[22] Mulliner, C., Golde, N., and Seifert, J. SMS of Death: From Analyzing to Attacking Mobile Phones on a Large Scale. In ***USENIX Security***, 2011.

[23] Sarma, B., Li, N., Gates, C., Potharaju, R., Nita-Rotaru, C., and Molloy, I.. Android permissions: a perspective combining risks and benefits. Paper presented at ***the 17th ACM Symposium on Access Control Models and Technologies***, pp. 13–22, 2012.

[24] Strazzere, T. Security Alert: zHash, A Binary that can Root Android Phones, Found in Chinese App Markets and Android Market. ***The Lookout Blog***, 2011.

[25] Theoharidou, M., Mylonas, A., and Gritzalis, D. (2012). A risk assessment method for smartphones. Paper presented at ***the 27th IFIP Information Security and Privacy Conference***. Springer (AICT 376), pp.443-456, 2012.