基於資料外洩的行動惡意程式行為分析

陳嘉玫　江玟璟　陳怡靜　張明達　吳惠麟　曾昭銘
台灣學術網路危機處理中心(TACERT)
chiamei.chen@gmail.com

摘要

行動裝置出現已經有一段時間，但其安全問題一直未受到大家注意，直到近來科技快速的進步下、行動裝置開始擁有不下於個人電腦的計算能力，越來越多人使用行動裝置進行各項活動，其中儲存的大量使用者資料，吸引了駭客們注意並對其開發並製作惡意軟體，這些惡意軟體以行動裝置上使用者資料為目標，造成使用者的資料外洩，被用來謀取利益，對使用者造成極大的損失。

本研究提出用敏感性資料洩露為特徵來偵測惡意程式的方法，利用封閉環境的模擬裝置來隔離並執行應用程式，透過行為分析的方式，監控並記錄應用程式執行過程中的行為，並對其相關行為進行深入分析，從檔案與網路連線等方面，來分析並追縱敏感性資料是否被送出行動裝置外面，同時也針對應用程式發送短訊息的行為是否異常等方式，來偵測惡意軟體。透過實際的惡意樣本進行實驗，結果證明在分辨惡意軟體的正確率上以及誤判率上各取得不錯的成果，比起現有的方式，像是以權限為基礎來進行分析或是透過系統呼叫繁率等方式，能夠擁有較好的惡意軟體偵測率，並擁有較低的誤判率。

關鍵詞：行動裝置安全、Android、行為分析、動態分析、惡意軟體偵測。

1. 前言

移動裝置又稱手持裝置，典型的裝置有個人數位助理、行動電話…等，隨著技術的進步、網路的普及，智慧型手機開始在市場上嶄露頭角，更整合行動電話和個人數位助理系統等，成為全方位的行動網上裝置，為了追求較好的效能與方便性，更出現平板電腦，漸漸形成個人與網際網路的不可分割性。這些移動裝置不只是能作為行動電話與朋友間聯絡之用、也可以用來上網、收發信件，以及進行娛樂影音用途。更甚之可以透過行動裝置來進行財務管理，也因為如此行動裝置上面儲存著大量的個人敏感資料，如：各類網站、信箱等服務之帳號密碼、個人通訊資料、金融轉帳資料等。這些重要的個資更吸引駭客們的注意，花費心思鑽研破壞行動裝置的安全性問題，透過獲取手機使用者的隱私資料、如通訊錄、個人資料，以及利用手機寄送付費簡訊或是進行不合法的行為，從中獲取利益。由於早期行動電話所使用的作業系統與應用程式，多由行動電話設備商自行開發或採取合作異同開發，因此不同手機所搭載的程式，具有相當大的差異性。對於這類型的裝置，較不受駭客青睞，因此早期手機的安全性問題較不受人們重視。

雖然近年來各家廠商已不斷改進行動裝置的安全性，但是從報告中可以發現，行動裝置的安全威脅不但沒有降低反而日益嚴重。目前除了官方的市場外還有第三方市場，對於開發者而言在第三方市場上發佈軟體是不需要付開發者費用的，吸引了部份開發者選擇在第三方市場上發佈軟體。這也導致了一些駭客利用這個方式散佈自己的惡意軟體。而一些使用者為了規避官方市場付費軟體的費用，選擇從第三方市場下載破解版本，結果反而下載到惡意軟體。有些熱門實用的軟體，官方只提供部份語言，使用者礙於語言障礙，透過第三方市場下載經過翻譯的版本，這也導致使用者可能下載到惡意軟體的風險。

目前應用於行動裝置的分析模式與基於個人電腦的分析方法類似，亦區分為靜態分析與動態分析兩種。靜態分析相較於動態分析，前者的優點在於不需要執行應用程式的情況下，透過程式的反組譯，由程式碼中找尋特徵值，分析時間短且快速、不會在分析期間造成感染擴散等問題。但缺點是，靜態分析必須能夠事先獲取其惡意程式特徵值，因此對於新威脅的應變能力較弱。此外，近來惡意程式使用了大量的程式碼混淆機制，造成靜態分析在解析程式碼上面臨困難。

動態分析方法的缺點是，因為需要執行應用程式來進行分析，在分析執行效率方面，則略遜於靜態分析。但是動態分析的優點則重於行為上的分析 ，即使攻擊者所採用的攻擊方式改變、使用新的漏洞或是利用混淆機制來阻礙分析，其惡意行為也不能夠被隱藏，因此在面對新的行動裝置平台上與新型態的攻擊模式上，動態分析比起靜態分析更能夠快速的應對這些安全威脅。

本研究利用現有動態分析，利用現有模擬裝置建置一個動態行為分析的系統平台。監控並記錄應用程式的行為，並對其相關行為進行分析，追縱應用程式執行過程資料的流向，來判斷良性與惡意程式。與現有重於權限與系統呼叫頻率的分析相比，能夠有效分辨良性與惡意程式，並擁有較低的誤判率。

2. 相關技術背景

2.1 行動裝置概況

近年來，智慧型手機開始出現，以蘋果(apple)公司所推出搭載 iOS 作業系統的 iPhone 智慧型手機谷哥(Google)公司所推出搭載 Android 作業系統的手機為市場的主流，其它還包括 Windows 的 Phone7 RIM 的 BlackBerry 等。根據 IDC 在 2012 年 5 月所公佈的統計數據[1]，如所示 Android 在 2012 年第一季市占率約 59%，緊接著 iOS 為 23%。為了推陳出新並迎合客戶的喜好，各家廠商各自釋出自己的 API，供程式人員開發相關行動裝置的應用程式，因此降低開發應用程式的難度，讓大多數的程式開發者可以共同參與開發應用程式的工作。在難度降低與多人使用的誘因之下，更是吸引大量的駭客的注意。

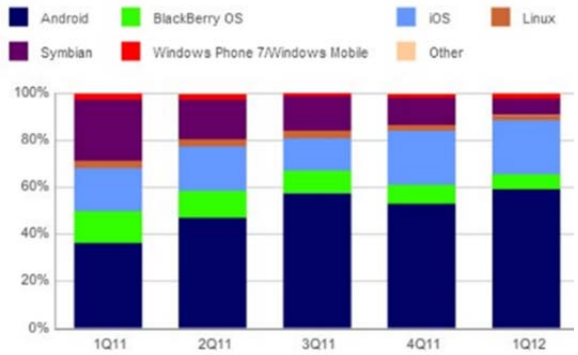


圖 1 全球行動裝置市佔率[1]

根據 McAfee2012 年威脅報告[2]指出，如圖 2 所示，McAfee 到 2012 年為止，其發展速度更是以幾何倍數的方式持續遞增成長。所收集的惡意樣本就高達了 8000 個，其樣本中有 7000 個屬於 Android 平台。如圖 3 所示，相較於其它平台來說 Android 的惡意軟體數量就佔了大部份，其次為諾基亞(Nokia)所使用的 Symbian 系統。

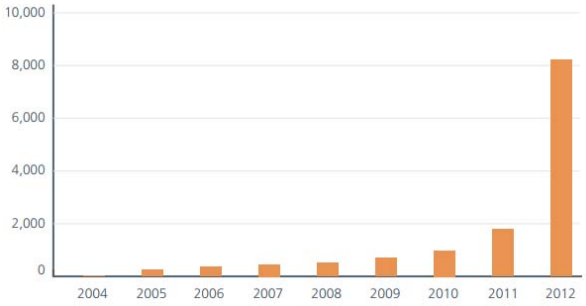


圖 2 行動裝置樣本數[2]

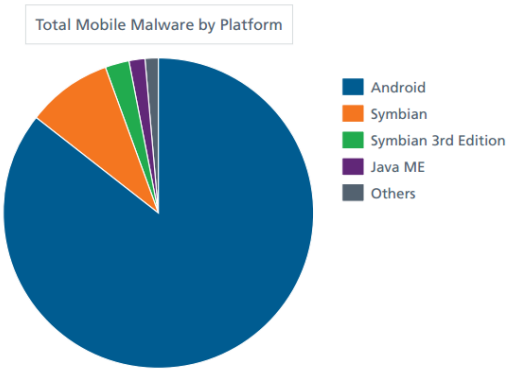


圖 3 平台樣本數[2]

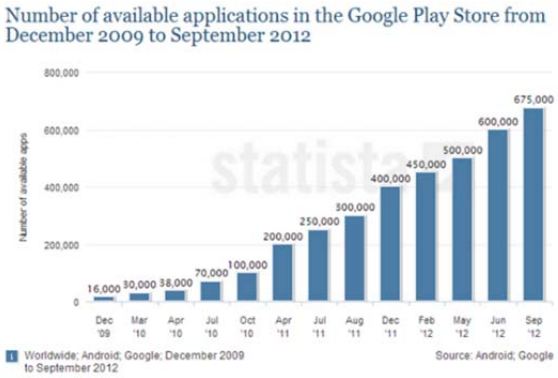


圖 4 Google Play 應用程式數量[3]

從 Google play 上的應用程式數量的增長率(圖 4)與惡意樣本數增長率相比，可以發現，應用程式數量從 2009 年 12 月的一萬六千個，到 2012 年 9 月的 67 萬個，呈現出倍數成長的趨勢，而惡意軟體樣本的增長率也自 2010 年起開始大幅度上升，到了 2012 年更是呈現爆炸性的增加。其原因可能是著眼於 2009 年 Google play 官方市場的正式營運並伴隨第三方市場的出現，Android 開放源碼的特性、語言上採用 java、使得開發與轉換平台難度降低，因此漸漸成為行動裝置的主流系統，駭客們也開始將攻擊重心轉往 android 平台，從而導致 2012 年惡意程式的數量大增。

2.2 惡意軟體

根據 F-Security 的 2013 第一季行動裝置威脅報告[4](如圖 5 所示)，可以發現 2011 年的惡意軟體種類中，以木馬程式的數量為最多，其次是病毒、蠕蟲與監視軟體等。報告指出，大量的惡意軟體會竊取行動裝置的資訊，包括行動裝置的國際行動識別碼、SIM 卡號碼、聯絡人資訊、作業系統資訊等，並透過簡訊服務(SMS，Short Message Service)、網路連線存取(如：透過網頁的 GET、POST)等方式將這些資料傳給遠端服務器或是利用被感染的手機發送付費 SMS、瀏覽網頁賺取點擊數等。

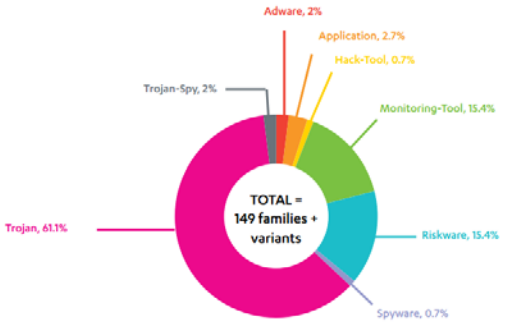


圖 5 惡意軟體種類[4]

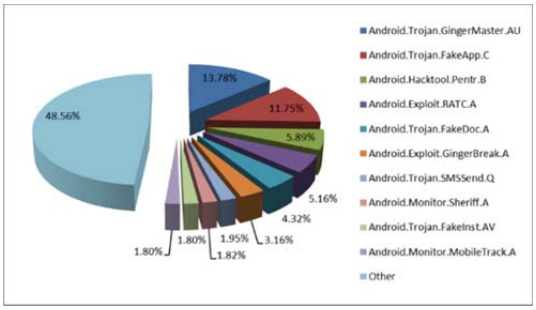


圖 6 前十大惡意軟體

如圖 6 所示，以前十大惡意軟體為例，像是偵測比例最大的 Android.Trojan.GingerMaster.AU 以及 Anroid.Trojan.FakeDoc.A 等木馬軟體，會收集使用者的行動裝置資料並傳送至遠端伺服器，造成使用者的資料外流並侵犯隱私。Android.Trojan.FakeApp.c 此木馬軟體，會顯現一些廣告讓使用者點擊之後，以賺取點閱數並秘密的收集使用者的資料。另外其它家族的 FakeAndroid.Trojan.SMSSend.Q 與 Android.Trojan.FakeInst.AV 則是會在使用者不知情的情況下，發送 SMS 訊息到付費號碼，來賺取使用者的金錢。

3. 系統架構

本系統的架構如圖 7 所示，共分為執行區塊(Execution Section)以及分析區塊（Analysis Section）兩大部份。Android 的.apk 檔案會送入執行區塊，這部份會進行模擬器的建置、啟用，並且進行應用程式的安裝與執行，隨後會對應用程式發出模擬操作行為，過程中應用程式在模擬器中的各種行為訊息會被記錄下來，同時會將所產生並被記錄下來的行為訊息傳送至分析區塊進行分析。分析區塊的部份本研究所提出的分析器（Analyzer）收到從執行區塊傳來的行為訊息記錄後會開始進行分析，如果行為訊息被辨識為惡意行為時，分析器會通知執行區塊中止執行階段，接著分析器會將訊息記錄進行統整後產生出行為分析報告（Behavior Report），此報告會顯示此應用程式是否有進行任何可疑的惡意行為，並根據其行為判斷是否為惡意程式。

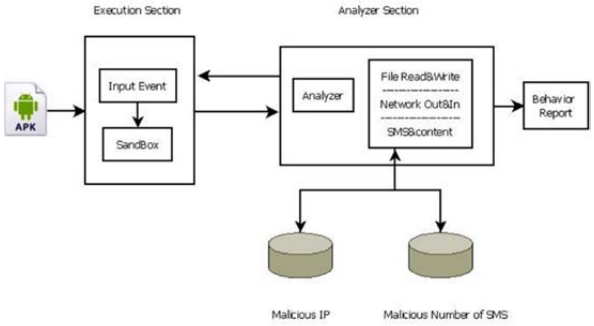


圖 7 系統架構

3.1 Execution Section

執行區塊（Execution Section）的部份主要被區分為兩個部分，（輸入產生器）Input Generator 以及（模擬器）Emulator 兩個區塊。進行分析的過程模擬器區塊會配置一個模擬器，當模擬器建置完成時，傳送過來的.apk 檔案會被送入模型器中，並進入安裝階段，此安裝過程與一般行動裝置上的安裝程序是相似的。當應用程式安裝完成一段時間後，輸入產生器區塊會開始對模擬器傳送輸入行為訊息，對應用程式自動產生輸入訊息以模擬使用者操作 Android 裝置的行為，藉此與應用程式進行互動。在模擬器運作的過程中，所有系統的訊息會被記錄下來，並同時傳送給分析區塊進行分析。

該虛擬機器每當執行完一個應用程式分析就會進行系統初始化的動作，分析結束時會將目前的虛擬機器刪除，在每次進行新的分析前會配置一個新的虛擬機器，以避免前次的實驗影響到本次實驗的結果而造成不必要的誤判。

3.2 Analysis Section

分析區塊(Analysis Section)部份的則有以下三個主要的分析重點：

- Read&Write
- Network Out&In
- SMS Content。

本研究的分析區塊是利用 Python 搭配 hell Script 共同篩寫而成，分析區塊會以上面三個部份為主要對象進行分析，其目的主要是在確認以上這三個部份有沒有出現惡意行為。執行區塊執行的期間，會不斷的將模擬器最新的行為記錄訊息傳到分析區塊區塊，每當分析區塊收到一筆行為記錄訊息，會將該行為訊息記錄傳至自行開發的分析器，會針對該行為記錄訊息以上三個部份進行分析，如果在行為記錄訊息中發現任何惡意的行為，分析器就會發出中止訊息停止執行區塊的運行，並對該應用程式的行為產生一份行為報告。之後會進行實驗環境的復原與初始化的動作，以供下一次的實驗進行。

要判斷是否有惡意行為，必須確認是否有將敏感性資料外洩的行為，行動裝置上的敏感性資料很多，依據其行動裝置規格與使用的應用軟體可能會

有差異，為了要鎖定重要的敏感性資料做為特徵，本研究除了前章所述研究所討論的敏感性資料，另外針對由相關研究單位 Android Malware Genome Project 與 contagion mobile 所提供的真實的惡意樣本進行研究、檢測與分析。所有的行動裝置都會共同擁有的資料為主，惡意應用程式會收集的目標進行探討，本研究定出四種敏感性資料（如表 1 所示）：

表 1 敏感性資料

名稱	敘述
國際移動設備辨識碼 (IMEI)	一般稱作行動裝置序列號、行動裝置唯一碼，由於每一個行動裝置都有其獨立的識別碼，因此又被稱為是行動裝置的身份證。其號碼的組成是由核准序號+產地序號+生產序號+檢驗序號組成。
國際移動用戶識別碼 (IMSI)	在電話網路中用來識別移動用戶的唯一識別碼，一般存在 SIM 卡中。由行動國家碼+行動網路碼+行動用卡識別碼組成。
系統訊息	各類系統裝置的訊息。如：系統版本、裝置型號等
通訊錄訊息	以往的行動裝置上又稱為電話簿，一般可以登記電話持有人的姓名、電話、住址、信箱等個人資訊。

File Read&Write 的部份，有部份的惡意程式會在執行的過程中，收集裝置上面的敏感性資訊並儲存在檔案中，如：xml 檔案。在應用程式執行的過程中在將存有敏感性資料的檔案傳送到遠端伺服器上。

分析重點：

- 追蹤帶有敏感性資料的檔案

Network In&Out 的部份，大部份的惡意程式會在對外網路連線過程中，透過各種方式將敏感性資料傳送到遠端伺服器。通常是以誘騙的方式或是在不通知使用者的情況下，在使用者操作應用程式的過程中，將敏感性資料藏在連線資料中傳送至遠端伺服器。

此外也有部份惡意程式會在程式的運行中誘導使用者操作下載其它的 APK 檔案。其方式有可能透過誘騙使用者該應用程式有新的更新可以使用，或是推薦使用者其它相似的工具來誘騙使用者下載，因此可能在原本的惡意程式中並沒有任何的惡意行為，但是下載的程式確會執行惡意行為。

分析重點：

- 惡意程式會在對外網路連結過程中，並將敏感性資料混入訊息中傳出。
- 惡意程式會在對外網路連結過程中，將含有敏感性資料的檔案向外傳輸。
- 惡意程式會在操作應用程式的過程中下載其它的 apk 檔案。

SMS Content 的部份，從樣本觀察中發現部份惡意程式會在傳送 SMS 訊息時，將該系統的敏感性資料混入 SMS 訊息中傳出。也有一些惡意程式雖然不進行傳送敏感性資料的行為，但是會以一些規律性的行為寄送付費的 SMS 簡訊，

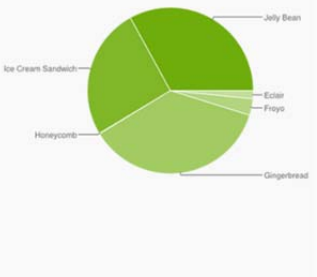
本研究再將以上的行為進行歸納，若有發生以下行為視同異常：

- 發送付費簡訊
  - 短時間內對不同號碼寄送兩封以上簡訊的行為。
  - 對同一個號碼發送簡訊兩次以上的行為。
- 發送的簡訊中會含有系統的敏感性資料。

4. 實驗

4.1 系統建置

Version	Codename	API	Distribution
1.6	Donut	4	0.1%
2.1	Eclair	7	1.5%
2.2	Froyo	8	3.2%
2.3 - 2.3.2	Gingerbread	9	0.1%
2.3.3 - 2.3.7		10	36.4%
3.2	Honeycomb	13	0.1%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	25.6%
4.1.x	Jelly Bean	16	29.0%
4.2.x		17	4.0%



Data collected during a 14-day period ending on June 3, 2013.
Any versions with less than 0.1% distribution are not shown.

圖 8 Android 平台版本分布

Android 以版本號來說共有四個版本，分別以 1、2、3 與 4 為開頭，部份版本帶有同樣的代號名稱。以平台來區分的話，android 的第 1 版與第 2 版是用於智慧型裝置，第 3 版則是用於平版裝置。而後 Google 為了將方便開發團隊開發，將兩類平台整合為第四版。如圖 8 所示，2013 年 1 月的統計顯示 android 裝置的版本以 Gingerbread(36.5%)、Ice Cream Sandwich(25.6%)以及 Jelly Bean(33%)此三個版本使用率較高，其中又以 GingerBread 所佔的比例最高。由於硬體裝置的限制，很多使用者並無法更新到新版本的 Android 裝置。此外 android 第 2 版與第 3 版的差異主要在於改進開發者平台與使用者介面

上的改進，因此本系統 android 模擬器將以 GingerBread 的版本來進行建置。

4.2 樣本

本研究在惡意樣本方面總共收集到 10 個家族共 135 個樣本，10 個家族的名稱與行為如表 2 所示：

表 2 惡意樣本家族列表

名稱	行為
AnserverBot	在 Android 裝置開啟後門竊取資料傳送到遠端服務器。
BaseBridge	竊取資料傳送到遠端服務器。
BeanBot	受 C&C 服務器控制寄送 SMS 訊息。
Bgserv	獲取使用者手機資訊傳送至特定網址。
DroidKungFu	收集大量訊息記錄在檔案中並傳送至遠端服務器。
GoldDream	竊取資料傳送到遠端服務器
HippoSMS	寄送付費簡訊並攔截簡訊訊息。
Pjapps	在 Android 裝置開啟後門竊取資料傳送到遠端服務器。
RogueLemon	竊取資料傳送到遠端服務器
plankton	受 C&C 服務器控制能夠下載、安裝程式、寄送 SMS 簡訊等。

本研究在良性樣本的取得方面，由於使用者可以取得 apk 檔案的地方不僅止於官方 Google play 市場，也可於其它第三方市場處下載。原本 Google play 市場採用的是使用者回報機制，也就是當使用者發現應用程式為惡意程式時，可以回報並檢舉該應用程式。不過，單憑如此的回饋機制還是不能阻止快速成長的 Android 惡意軟體，因此 2012 年 2 月 Google 在保留原本的回報機制時，另外推出代號為 Bouncer 的安全服務[5]，該服務會在應用程式被遞交至 Google Play 時對應用程式進行分析，其範圍是針對已知的惡意軟體、間諜軟體與木馬程式。

為了盡量避免下載的樣本是遭受污染、惡意的 ，本研究選擇 Google Play 市場上的應用程式做為良性樣本來源，在 Google Play 的市場上應用程式有被分門別類，如表 3 所示。本研究在在各類別中各下載數個應用程式，並只選擇被其它使用者評價為四星等以上的熱門應用程式(最高為五星等)，作為本研究的良性樣本來源。

表 3 良性應用程式類別

交通運輸	新聞與雜誌
個人化	旅遊與地方資訊
健康塑身	漫畫
動態桌布	生活品味
商業	生產應用
圖書與參考資源	社交
天氣	程式庫與試用程式
娛樂	財經
媒體與影片	購物
小工具	通訊
工具	運動
攝影	醫療
教育	音樂與音效

4.3 評估

為評估本系統的在真實情況下的分類效能，我們與 Right Alert 及 Permission Friendly 兩個系統做效能評估分析。我們採用各 135 個惡意及 135 個良性應用程式作為系統測試的樣本，合計共 270 個樣本。

在惡意樣本的偵測率表現如表 4 所示，總計 135 個的惡意程式樣本，Right Alert 將 118 個樣本判別為高風險程式，其惡意判別率有約為 87%。Permission Friendly 將其中 120 個樣本判為高風險程式，其惡意判別率為 88%左右。本系統在 135 惡意樣本中成功視別出 123 個樣本，惡意判別率約為 91%。在惡意漏報率方面，Right Alert 誤判 17 個惡意軟體，約有 12%的惡意漏報率，Permission Friendly 誤判了 15 個惡意軟體，約有 11%的惡意漏報率。本系統則是誤判 12 個軟體，惡意漏報率約為 8%。

本研究在惡意程式偵測方面，約有 8.89%的樣本被誤判成良性軟體，重新手動檢視這些樣本後發現，以 BeanBot 家族為主產生的誤判率較高，8 個樣本中僅認出一個樣本，檢閱 BeanBot 的相關資料，他的行為有向遠方伺服器傳送行動裝置資料或是接收 C&C server 來發送惡意簡訊的行為。經過手動檢查樣本後，可以知道這些程式是偽裝成系統工具讓使用者可以進行應用程式掃描並進行刪除的動作，在操作過該應用程式之後，並沒有產生任何惡意或可疑的行為，有可能是因為 C&C Server 已停止運作，程式在沒有收到命令的情況下並不會執行任何的惡意行為，因此本系統造成了誤判。

在良性樣本的判別率表現如表 5 所示，Right Alert 在 135 個良性樣本中，將 73 良性樣本視別為高風險軟體，良性判別率僅 45%而惡意誤報率達到 54%，而 Permission Friendly 在 135 個良性樣本中，將 109 個樣本視為高風險軟體，良性判別率僅 19%惡意誤報率達到 81%。而本研究在 135 個良性樣本中，將約 10 個樣本視為惡意軟體良性判別率約有 92%惡意誤報率僅約為 7%左右。本系統在分辨良性與惡意程式上擁有較有效的能力。

其全部樣本偵測率如**錯誤! 找不到參照來**

源。6 所示，Right Alert 的分析其準確率為 66%，Permission Friendly 其準確率僅 54%，相較之下，本研究的準確率有 91%，而錯誤率僅約 9%。Right Alert 與 Permission Friendly 是透過權限為基礎來進行風險評估的，接觸到越多行動裝置系統資訊的權限或是與傳送資料有關的權限，這樣都視為是高風險的權限，因為應用程式在擁有這些權限的情況下，例如：讀取行動裝置訊息、網路存取、修改記憶卡等權限，可能造成安全風險較高，因而導致其風險分數偏高。但是在一般的應用程式上，這些權限可能也是程式運行所需要的基本權限，所以在良性樣本的判斷方面，會造成誤判率較高，無法有效做為區分。

本系統在良性程式偵測方面，重新檢視了 10 個被歸類為惡意程式的樣本，發現這些被歸類為惡意程式的應用程式，對外傳送了行動裝置的 IMEI 碼，但是在應用程式的規章中並沒有說明或記載外傳使用者的 IMEI 碼。這些 IMEI 碼在使用者不知情的情況下被廠商用來辨識行動裝置，也沒有透過任何的雜湊加密，這些風險軟體可能會在特定的情況下會造成使用者的資料外洩。

表 4 惡意樣本偵測率

名稱	惡意 (高風險)	良性	TPR	FNR
Right Alert	118	17	87.41%	12.59%
Permission Friendly	120	15	88.89%	11.11%
Proposed	123	12	91.11%	8.89%

表 5 良性樣本偵測率

名稱	惡意 (高風險)	良性	TNR	FPR
Right Alert	73	62	45.93%	54.07%
Permission Friendly	109	26	19.26%	81%
Proposed	10	125	92.59%	7.41%

註:TNR(True Negative Rate)、FPR(False Positive Rate)

表 6 全部樣本偵測率

名稱	惡意 (高風險)	良性	TPR	FNR
Right Alert	191	79	66%	34%
Permission Friendly	229	41	54%	46%
Proposed	133	137	91%	9%

註:TPR(True Positive Rate)、FNR(False Negative Rate)

5. 結論

本研究利用駭客們攻擊行動裝置的最大動機－竊取使用者的資料，透過追縱敏感性資料是否被傳出行動裝置的方式，以區分良性與惡性程式。從結果來說，不論是在區分惡意程式與良性判別方面都取得九成以上的正確率，與舊有的以權限為基礎等研究相比較，不僅能夠更加準確的偵測惡意程式，以往研究在良性樣本上面臨的高誤判率也能夠有效的降低。此外，相較以往動態分析需要報行並收集 10 分鐘以上的系統資訊才能夠進行分析，本系統在執行時間約 3 分鐘左右，就能夠分辨良性或是惡意程式。

在現行平台發展不建全，規章限制不完全的情況下，即使是一般的程式也能夠在不通知使用者的情況下，自由取得使用者行動裝置的資料(在適當的權限下)。此外，開發人員為了開發上的方便直接使用行動裝置機碼來識別使用者或是為了評估自身產品的效益而私底下收集使用者的資訊，在沒有經過適當保護的情況下(如：雜湊加密)，就可能會形成安全上的疑慮，而這些風險軟體也是行動裝置上另一個要解決的問題。 在建置環境方面，現行的 Android 模擬器版本相當多，各個應用程式所需要的套件並不大相同，即使是 Google 官方推出的模擬器也不一定能順利執行每個應用程式，這將使得建置模擬器上出現障礙無法使用同一規格的模擬器來進行測試，使得行為分析平台受到限制。

行動裝置出現的時間雖然不長，但是在近年來硬體科技進步下，行動裝置出現了極大的改變，所以也面臨像電個人電腦般一樣的網路安全問題。行動裝置除了面臨舊有傳統威脅外，也出現屬於該設備才有的網路安全問題。在面對舊有威脅上受限於行動裝置的限制，多數威脅並不能套用傳統的解決方法。同時，新的威脅不斷的出現，對於行動裝置更是一大考驗。在行動裝置上與惡意程式對抗的路還有很長的一段要走，除了各單位在分析與偵測方面的改進以外，也期許行動裝置能夠建立更建全的開發規章來規範開發者，在兩方共進的情況下才能避免更多的惡意程式誕生。

參考文獻

[1] IDC, “Android and iOS Combine for 91.1% of the Worldwide Smartphone OS Market in 4Q12 and 87.6% for the Year , According to IDC ", available at: http://www.idc.com/getdoc.jsp?containerId=prUS23946013, 2012.

[2] McAfee, “McAfee Threats Report:First Quarter 2012”, 2012.

[3] Statista, “Number of available applications in the Google Play Store”, available at: http://www.statista.com/, 2012.

[4] F-Security, “MobileThreatReport Q1 2013”, 2013.

[5] H.Lockheimer, “Android and Security”, available at: http://googlemobile.blogspot.tw/2012/02/android-and-security.html, 2012