智慧型手機安全測試方法

林佑安 林盈達

國立交通大學資訊工程學系

Email: andylin.cs03g@nctu.edu.tw, ydlin@cs.nctu.edu.tw

September 15, 2014

摘要

近年來，資安議題已經不限於病毒入侵的問題，有心人士開始利用看似合法的需求，實際上卻收集個人資料等動作，所以本文將利用三種方式來測試智慧型手機內應用程式的安全性以及合法性，包括特徵碼掃描、權限瀏覽以及網路行為分析，並利用所提及的測試方法對市面上販售的紅米 Note 以及 Samsung GALAXY S III 進行測試，從測試結果發現在特徵碼分析中兩款智慧型手機各發現一個偵測異常的應用程式；權限瀏覽中發現紅米 Note 共有 128 個內建應用程式，其中含有 34 個疑似越權的應用程式，Samsung GALAXY S III 則共有 210 個當中含有 63 個疑似越權的應用程式；在網路行為分析中，並未發現 Samsung GALAXY S III 有傳輸個人資料到特定伺服器中，紅米 Note 則會在未經使用者授權將手機號碼、IMEI 號碼、應用程式列表等傳輸至特定的伺服器中。

關鍵字：手機安全、Android、資訊安全、封包分析、權限分析、特徵碼分析

1. 簡介

由於 CPU 的進步、硬體體積縮小以及 3G 網路的普及，智慧型手機漸漸在手機市場中嶄露頭角，使用智慧型手機收發電子郵件、觀看股票最新動態、透過攝影機進行視訊會議、利用 GPS 系統搭配地圖程式功能來規劃旅遊路線、上網查看各個景點的網友評價及多媒體等應用讓使用者隨時隨地享受流行脈動；從前要透過電腦才能做到的，現在在智慧型手機上都可以完成。也因為如此，有心人士也開始利用智慧型手機的系統或是應用程式的漏洞進而取得手機主控權或是取得個人隱私資訊(privacy information)等違法行為。最近在各大新聞中，播報了一些關於手機資安的報導，大則整個系統；小則應用程式，例如：小米手機未經使用者授權將個資傳至伺服器[1]、手機廠商 Star 所出廠的 N9500 內建間諜軟體[2]、Android 系統上有 Fake ID 之漏洞[3]等。此外，由於智慧型手機資安問題如雨後春筍般出現，台灣國家通訊傳播委員會(NCC)也將在未來建立手機系統資安檢測機制[4]，以降低智慧型手機資安問題的發生。

在本文章節中，首先第二節將介紹國外三個組織所提出的智慧型手機風險，並且將手機風險分類並討論；第三節我們將介紹三種測試方式，包括特徵碼(signature)掃描、權限(permissions)瀏覽以及網路行為(network behavior)分析；第四節則說明測試方式的實驗流

程；第五節將利用三種測試方式對市面上販售的紅米 Note 以及 Samsung GALAXY S III 進行測試並說明實驗結果；第六節則為本文做出總結。

2. 智慧型手機風險介紹

開放 Web 軟體安全計畫(Open Web Application Security Project, OWASP)、歐盟機構網路與資訊安全(European Union Agency for Network and Information Security, ENISA)、NetSafe 分別公布 Top 10 Mobile Risks[5]、Top Ten Smartphone Risks[6][7]以及 Smartphone Security Report 2014[8]，上述各組織所提及到風險於表一中呈現。在各組織所提及的手機風險中，包括了伺服器因素、程式因素、傳輸因素以及人為因素。當中人為因素占為多數，其次是程式因素，再者傳輸因素，最少是伺服器因素。

表一：各組織所提及到手機風險

報告名稱	內容
OWASP Top 10 Mobile Risks[5]	O1: Weak server side controls O2: Insecure data storage O3: Insufficient transport layer protection O4: Unintended data leakage O5: Poor authorization and authentication O6: Broken cryptography O7: Client side injection O8: Security decisions via untrusted inputs O9: Improper session handling O10: Lack of binary protections
ENISA Top Ten Smartphone Risks[6][7]	E1: Data leakage resulting from device loss or theft E2: Unintentional disclosure of data E3: Attacks on decommissioned smartphones E4: Phishing attacks E5: Spyware attacks E6: Network Spoofing Attacks E7: Surveillance attacks E8: Diallerware attacks E9: Financial malware attacks E10: Network congestion
NetSafe Smartphone Security Report 2014[8]	N1: Physical loss N2: Malware N3: Phishing N4: Smishing N5: Wi-Fi network spoofing N6: Privacy concerns (ex. GPS)

上述所提及風險之伺服器因素，說明可能在伺服器上出現弱點，使有心人士對伺服器攻擊以獲取所需的資訊(表一：O1)；傳輸因素，說明未使用加密方式傳送資料，可能將遭到被攔截或是被竊聽封包，導致資料外洩(表一：O3、E10)；人為因素，說明使用者可能會因遺失智慧型手機、汰換手機未銷毀個人資料、下載惡意程式、下載間諜程式、網路釣魚、簡訊釣魚、連線至不確定的 Wi-Fi 熱點造成資料外洩(表一：E1、E3、E4、E5、E6、E7、E8、N1、N2、N3、N4、N5)；程式因素，說明程式可能因未將資料加密保護、驗證

過於簡單、敏感資料寫至程式碼當中或是程式出現漏洞等因素，導致資料外洩或是有心人士的攻擊(表一：O2、O4、O5、O6、O7、O8、O9、O10、E2、E9、N6)。

在程式因素方面可以分成兩類，一為作業系統因素，二為應用程式因素。作業系統在開發時，因為疏忽注意某些事情，導致產生漏洞，例如近期公布的 Fake ID[3]、Masterkey[9][10]等。在應用程式因素中，包含了應用程式的漏洞以及被有心人士植入惡意程式的應用程式，皆可能造成智慧型手機的風險；而應用程式可分為內建應用程式、官方認證應用程式、非官方認證應用程式三類，當中內建應用程式為手機製造廠商在智慧型手機上預先安裝的應用程式，包括：通訊功能應用程式、手機廠商與合作廠商所提供服務的應用程式，且這類應用程式無法由使用者自行移除；官方認證應用程式為 Google Play、App Store 等官方市場所提供的應用程式，此類的應用程式需要通過官方的審核，才可上架至官方市場並開放下載，所以官方市場內的應用程式僅有少數藏有惡意程式至其中。非官方認證應用程式獲得管道有許多種，例如：第三方應用程式市集、網路下載的 apk 檔案等，此類應用程式因為沒有經過官方審核，較有可能隱藏惡意程式在其中，導致個人隱私資料洩漏、暗中進行手機小額付款等事件發生。

由於官方認證應用程式以及非官方認證應用程式為使用者自行決定是否要安裝此應用程式，本文將不討論此二類應用程式。而內建應用程式，使用者較容易忽略其資訊安全風險問題，主要是因為確信手機廠商不會安裝惡意軟體至手機內。但最近資安事件指出出廠手機內建間諜軟體，導致使用者對智慧型手機產生不信任感，因此本文將針對智慧型手機內建應用程式進行研究並且測試是否有資安疑慮的問題。

3. 測試方法

本文測試方法有三種，分別為特徵碼掃描、權限瀏覽以及網路分析行為。特徵碼掃描可以作為初步判斷應用程式是否為惡意程式或是含有病毒；權限瀏覽可以找出疑似越權的應用程式；網路行為分析則是可以找出應用程式可疑的網路行為，例如讀取可疑網站、傳遞個人隱私資料等行為。

特徵碼掃描

特徵碼掃描將利用 Dr. Web v.7 Anti-virus Light[11]、Malwarebytes Anti-Malware[12]兩個掃描病毒之應用程式以及線上病毒掃描器-Virustotal[13]進行特徵碼掃描，Dr. Web v.7 Anti-virus Light 可以選定範圍掃描檔案或是針對已安裝應用程式(包含內建應用程式)進行掃描，判斷其是否為惡意程式或是藏匿病毒在其中；Malwarebytes Anti-Malware 可以掃描出 Android 系統上已知的漏洞以及掃描應用程式(包含內建應用程式)是否為惡意程式。Virustotal 為線上病毒掃描器，裡面超過 50 個防毒軟體，使用者可上傳檔案進行掃描，掃描完成後即顯示偵測率以及結果報告。本文將利用以上三樣工具，進行智慧型手機整體掃描與內建應用程式的 apk 檔進行掃描是否為惡意程式或是藏匿病毒至其中。

權限瀏覽

權限瀏覽將利用 Permission Explorer[14]瀏覽每個應用程式的權限，因此我們可以列出有疑似取得本身不必要權限(以下簡稱越權)的應用程式。表二為本文將要進行瀏覽的權限，包含有資安疑慮以及可以改變系統設定的權限兩類。有資安疑慮的權限共有 19 項，包含位置讀取、帳號管理、簡訊管理、個人資料管理、聯絡人管理、錄音管理、相機管理、撥打電話、下載管理、讀取 LOG 資料等權限；可以改變系統設定的權限共有 5 項，包含重新啟動裝置、改變手機狀態、更改設定等權限。

表二：權限瀏覽列表

分類	權限	
有資安疑慮	ACCESS_COARSE_LOCATION ACCESS_FINE_LOCATION CALL_PHONE CALL_PRIVILEGED CAMERA DOWNLOAD_WITHOUT_NOTIFICATION GET_ACCOUNTS MANAGE_ACCOUNTS READ_CONTACTS READ_LOGS	READ_PROFILE READ_SMS RECEIVE_SMS RECORD_AUDIO SEND_SMS SEND_SMS_NO_CONFIRMATION WRITE_CONTACTS WRITE_PROFILE WRITE_SMS
可以改變系統設定	DEVICE_POWER MODIFY_PHONE_STATE REBOOT	WRITE_APN_SETTINGS WRITE_SECURE_SETTINGS

網路行為分析

網路行為分析將利用 Wireshark[15]擷取並分析經由 Wi-Fi 傳輸的封包是否有傳送個人隱私資料至特定的伺服器中。

4. 實驗流程

特徵碼掃描

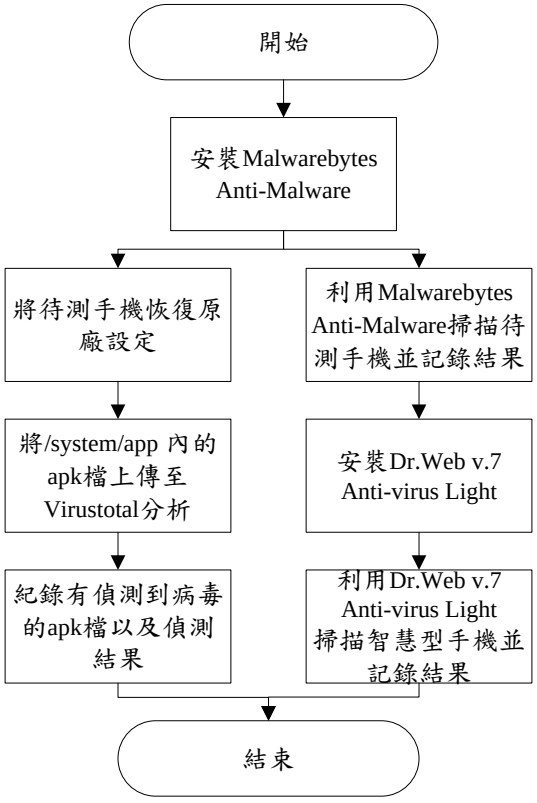
圖一為特徵碼掃描之實驗流程圖。先將待測手機恢復原廠設定，接下來安裝 Dr. Web v.7 Anti-virus Light 以及 Malwarebytes Anti-Malware 至手機內，並掃描待測手機，最後紀錄掃描結果。另外，並將/system/app 目錄內的 apk 檔上傳至 Virustotal 掃描，並記錄有偵測到病毒之 apk 檔及其掃描結果。

權限瀏覽

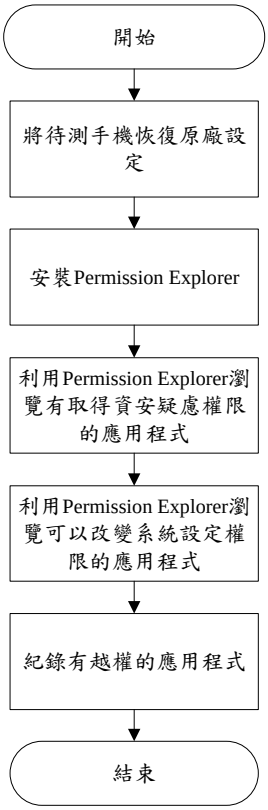
圖二為權限瀏覽之實驗流程圖。先將待測手機恢復原廠設定，並安裝 Permission Explorer，接下來利用 Permission Explorer 瀏覽需要取得有資安疑慮或是可以改變系統設定權限的應用程式，並把有越權的應用程式紀錄下來。

網路行為分析

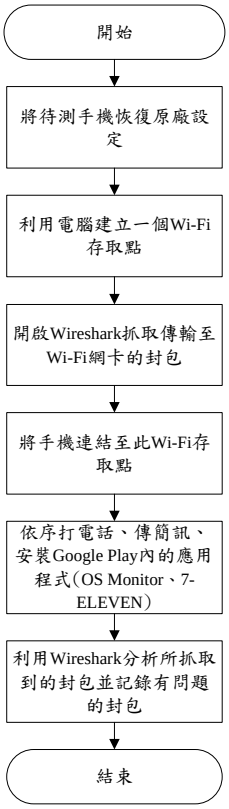
圖三為網路行為分析之實驗流程圖。先將待測手機恢復原廠設定，並連結至電腦所建立的 Wi-Fi 存取點，並利用 Wireshark 抓取通過 Wi-Fi 網卡的封包，接著將待測手機依序打電話、傳簡訊、安裝 Google Play 內的應用程式(OS Monitor、7-ELEVEN)，最後利用 Wireshark 分析所抓取到的封包，並將有傳送電話號碼、手機識別碼、帳戶資料等有關個人資訊的封包紀錄下來。



圖一：特徵碼掃描流程圖



圖二：權限瀏覽流程圖



圖三：網路行為分析流程圖

5. 實驗結果

環境介紹

本實驗將利用紅米 Note 以及 Samsung GALAXY S III(以下簡稱為 S3)作為實驗手機，圖四以及圖五為各手機系統資訊圖。紅米 Note 的 Android 版本為 4.2.2、MIUI 版本為 MIUI-JHDMIBF28.0；S3 的 Android 版本為 4.1.2、版本號碼為 JZO54K.I9300ZSEMK3。紅米 Note 版本為小米公司尚未更新網路簡訊自動開啟之版本，也是首次小米手機被發現有資安疑慮的版本。

圖四：紅米 Note 手機系統資訊圖

圖五：S3 手機系統資訊圖

特徵碼掃描

表三為紅米 Note 以及 S3 特徵碼掃描結果比較表，可以發現在兩款手機利用 Dr.Web v.7 Anti-virus Light 以及 Malwarebytes Anti-Malware 掃描整個手機裝置後皆沒有發現到任何一個應用程式有異常狀態，但將手機內建應用程式的 apk 檔上傳至 Virustotal 掃描後，各發現有一個 apk 檔被偵測到異常，分別為 GuardProvider.apk 以及 DreyeforSamsung.apk。GuardProvider.apk 為紅米 Note 內建的騰訊手機管家模組，此為提供手機安全的防護，例如病毒掃描的服務。GuardProvider.apk 掃描結果如表四，可以發現共有 54 個防毒軟體掃描此檔案，有 9 家防毒軟體掃描出有異常，其中有 3 家防毒軟體掃描出有 Android 的 Trojan 病毒。DreyeforSamsung.apk 為 S3 內建的 Dr.eye 字典應用程式，掃描結果如表五，共有 55 個防毒軟體掃描此檔案，只有 NANO-Antivirus 掃瞄出有 Android 的 Trojan 病毒。

表三：紅米 Note 以及 S3 特徵碼掃描結果比較表

	紅米 Note	S3
Dr.Web v.7 Anti-virus Light	無發現異常	無發現異常
Malwarebytes Anti-Malware	無發現異常	無發現異常
Virustotal	共掃描 103 個 apk 檔，其中 GuardProvider.apk 被偵測到有異常，偵測率：9/54	共掃描 209 個 apk 檔，其中 DreyeforSamsung.apk 被偵測到有異常，偵測率：1/55

表四：GuardProvider.apk 掃描結果表

名稱	GuardProvider.apk	
偵測率	9/54(表示 54 個防毒軟體有 9 個防毒軟體偵測出有異常)	
結果報告	Antivirus	Result
	AVware	Trojan.AndroidOS.Generic.A
	AntiVir	SPR/ANDR.SmsReg.AM.Gen
	Baidu-International	Hacktool.Android.SMSreg.BGT
	ESET-NOD32	a variant of Android/SMSreg.GT
	McAfee	Artemis!BEBB7A349697
	McAfee-GW-Edition	Artemis!BEBB7A349697
	NANO-Antivirus	Trojan.Android.Agent.daomfb
	TrendMicro-HouseCall	Suspicious_GEN.F47V0620
	VIPRE	Trojan.AndroidOS.Generic.A
SHA256	6b72e49bc9dea3b0d51d9a9614241594a29d16c9ef9f7acc1154083cd5517b80	

表五：DreyeforSamsung.apk 掃描結果表

名稱	DreyeforSamsung.apk	
偵測率	1/55	
結果報告	Antivirus	Result
	NANO-Antivirus	Trojan.Android.Banker.dcrgjd
SHA256	30665a585edc714ec477410d439562eb13483cae0570e6f1b0cb28a4a86cf266	

權限瀏覽

附錄一以及附錄二為紅米 Note 以及 S3 的權限瀏覽結果報告表，紅米 Note 內建應用程式有 128 個中，有 34 個疑似有越權的應用程式，S3 則是 210 個內建應用程式中有 63 個疑似越權的應用程式。兩隻待測手機共有 12 個應用程式皆有疑似越權的疑慮，但在各個手機上所要求的權限卻不一樣，例如：com.android.email 在紅米 Note 需要 DOWNLOAD_WITHOUT_NOTIFICATION，但在 S3 卻不需要此權限而是需要 ACCESS_COARSE_LOCATION、ACCESS_FINE_LOCATION、READ_SMS、RECEIVE_SMS、SEND_SMS、WRITE_SECURE_SETTINGS 這六個權限，可以發現雖然一樣的應用程式，卻需要的權限卻不相同，極有可能資安問題就藏在此應用程式中。

網路行為分析

在網路行為分析中，紅米 Note 與 S3 有不同的結果，S3 傳輸至 Samsung 伺服器的訊息並沒有發現到傳輸個人資料在其中。相反的，紅米 Note 在網路行為分析中發現，在未經

授權下會將個人資料，例如手機號碼、IMEI、應用程式列表傳送至小米伺服器中，相關實驗結果如以下說明。

表六與表七為紅米 Note 網路行為分析表，在未插手機 SIM 卡時，首先會先傳手機所安裝的應用程式清單至伺服器中，也有利用 SSL 傳輸資料至 register.xmpush.xiaomi.com，也有利用 XML 方式傳輸資料至 58.68.235.232，並沒有發現可疑的資訊。接著傳輸瀏覽器的常用書籤至 api.browser.miui.com/bsr/update/quicklinks4，但在第二次測試(插手機 SIM 卡中)卻沒有發現傳輸瀏覽器常用書籤至指定網頁中，如圖八的封包比較。

將手機 SIM 卡插入紅米 Note 後，首先會去下載多組門號的資訊至手機中，其中包括英國、大陸、台灣、印度、香港、菲律賓等國家電話號碼，該門號是小米公司傳送簡訊之門號，如圖九、圖十所示。接下來會將手機所安裝的應用程式清單至伺服器中，而實驗結果顯示若有安裝新的應用程式將會再重新傳送一次，如圖十一的封包比較圖所示。另外，傳送至 58.68.235.232 的 XML 封包，若插上手機 SIM 卡後，會傳送本機的手機號碼至 xiaomi.com 此伺服器中，如圖十二所示。另外，在使用者傳送簡訊時，紅米 Note 會將手機的 IMEI 號碼以及接收者的手機號碼傳輸至 api.account.xiaomi.com/pass/v3/user 內，如圖十三所示，小米公司解釋是為了確認雙方是否可以使用小米手機內建的免費網路簡訊功能，需傳輸 IMEI 以及接收者手機號碼進行確認，並說明使用者可以將免費網路簡訊功能關閉，手機即不傳送相關資訊至伺服器中，但手動將免費網路簡訊功能關閉後，IMEI 號碼以及接收者手機號碼卻依然傳送至伺服器中。另外，在表七中的順序 4、6、15，皆是疑似有傳輸裝置資訊至該伺服器中，由於傳輸內容皆是亂碼，無法利用比較字元方法進行確認是否有傳輸裝置資訊，但由標籤來判斷將極有可能為裝置資訊，如圖十四所示。

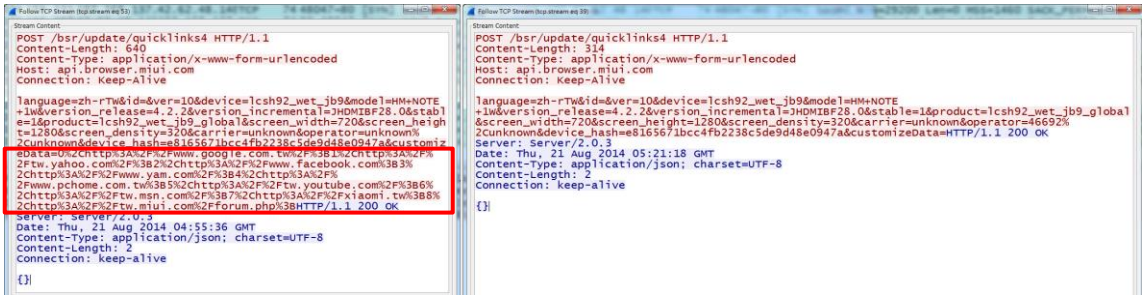
表六：紅米 Note 行為分析表(未插手機 SIM 卡)

順序	資訊	網址
1	傳送應用程式清單	http://policy.app.xiaomi.com/cms/interface/v1/checkpackages.php
2	利用 SSL 傳輸資料	https://register.xmpush.xiaomi.com
3	利用 XML 傳輸資料	58.68.235.232
4	利用 XML 傳輸資料	58.68.235.232
5	傳了瀏覽器的常用書籤	http://api.browser.miui.com/bsr/update/quicklinks4

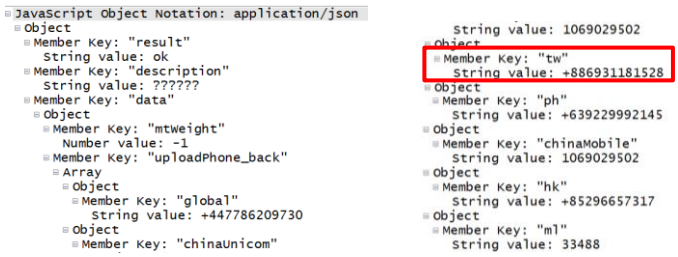
表七：紅米 Note 行為分析表(有插手機 SIM 卡)

順序	資訊	網址
1	下載內容中有一些門號	http://api.account.xiaomi.com/pass/configuration
2	傳送應用程式清單	http://policy.app.xiaomi.com/cms/interface/v1/checkpackages.php
3	利用 SSL 傳輸資料	https://register.xmpush.xiaomi.com
4	疑似傳輸裝置資訊	http://ac.account.xiaomi.com/pass/activation/getPhoneBySimIdDevId

5	利用 XML 傳輸資料，封包中有傳輸本機電話號碼	58.68.235.232
6	疑似傳輸裝置資訊	http://ac.account.xiaomi.com/pass/activation/safe/createOrUpdateUser
7	利用 SSL 傳輸資料	https://account.xiaomi.com
8	利用 XML 傳輸資料，封包中有傳輸本機電話號碼	58.68.235.232
9	傳送 IMEI 以及發送簡訊的電話號碼	http://api.account.xiaomi.com/pass/v3/user@id?type=MXPH&externalId=983xxxxxx
10	傳送 IMEI 以及發送簡訊的電話號碼	http://api.account.xiaomi.com/pass/v3/user@id?type=MXPH&externalId=983xxxxxx
11	(此時間點為發送簡訊)	
12	(此時間點為登入小米雲)	
13	利用 SSL 傳輸資料(應為帳號登入資訊)	https://account.xiaomi.com
14	利用 SSL 傳輸資料	https://open.account.xiaomi.com
15	疑似傳輸裝置資訊	http://ac.account.xiaomi.com/pass/passportapi/safe/getPhoneTicket?sid=kbPPB3iP97bi5JxOpnyfng%3D%3D&devId=yqW8yj8XGreD1hYaSJO8NJ3KhWhOBQ33KPpO5zR3lOA%3D&phoneSimIdPair=a%2FgIIUZCVZYTnyM2NbHZOcblifjoUYrAoLwnOG7y
16	利用 SSL 傳輸資料(應為帳號登入資訊)	https://account.xiaomi.com
17	傳送 IMEI 以及發送簡訊的電話號碼	http://api.account.xiaomi.com/pass/v3/user@id?type=MXPH&externalId=983xxxxxx
18	傳送 IMEI 以及發送簡訊的電話號碼	http://api.account.xiaomi.com/pass/v3/user@id?type=MXPH&externalId=983xxxxxx
19	**(此時間點為發送簡訊)**	
20	利用 XML 傳輸資料，封包中有傳輸本機電話號碼	58.68.235.232
21	**(此時間點為開始登入 GOOGLE 帳號)**	
22	傳送應用程式清單	http://policy.app.xiaomi.com/cms/interface/v1/checkpackages.php
23	**(此時間點安裝完成 OS Monitor)**	
24	傳送應用程式清單	http://policy.app.xiaomi.com/cms/interface/v1/checkpackages.php
25	**(此時間點安裝完成 7-ELEVEN)**	
26	傳送應用程式清單	http://policy.app.xiaomi.com/cms/interface/v1/checkpackages.php
27	傳送應用程式清單	http://policy.app.xiaomi.com/cms/interface/v1/checkpackages.php
28	利用 XML 傳輸資料，封包中有傳輸本機電話號碼	58.68.235.232

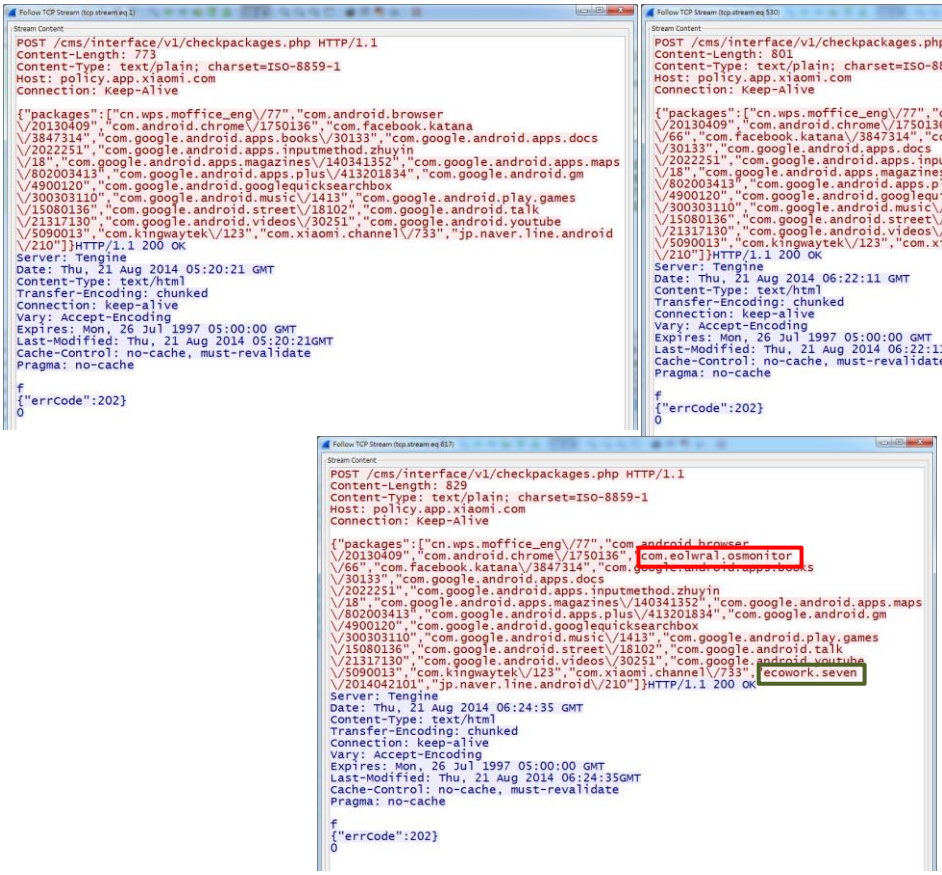


圖八：封包比較圖(左為未插手機 SIM 卡有傳送瀏覽器書籤資訊，右為插手機 SIM 卡未傳送資訊)



圖九：下載各地電話之封包

圖十：小米公司發送簡訊手機門號

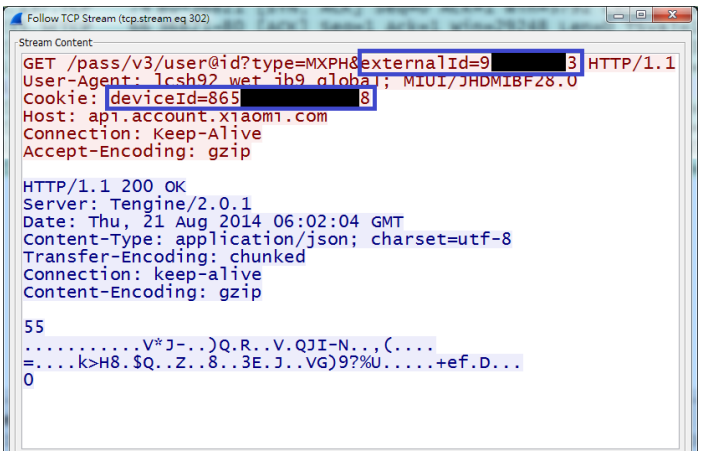


圖十一：傳送安裝的應用程式封包比較圖(左上為第一次傳送內容；右上為第二次傳送內容，多 OS Monitor 應用程式資訊；下為第三次之後傳送內容，多 7-ELEVEN 應用程式資訊)

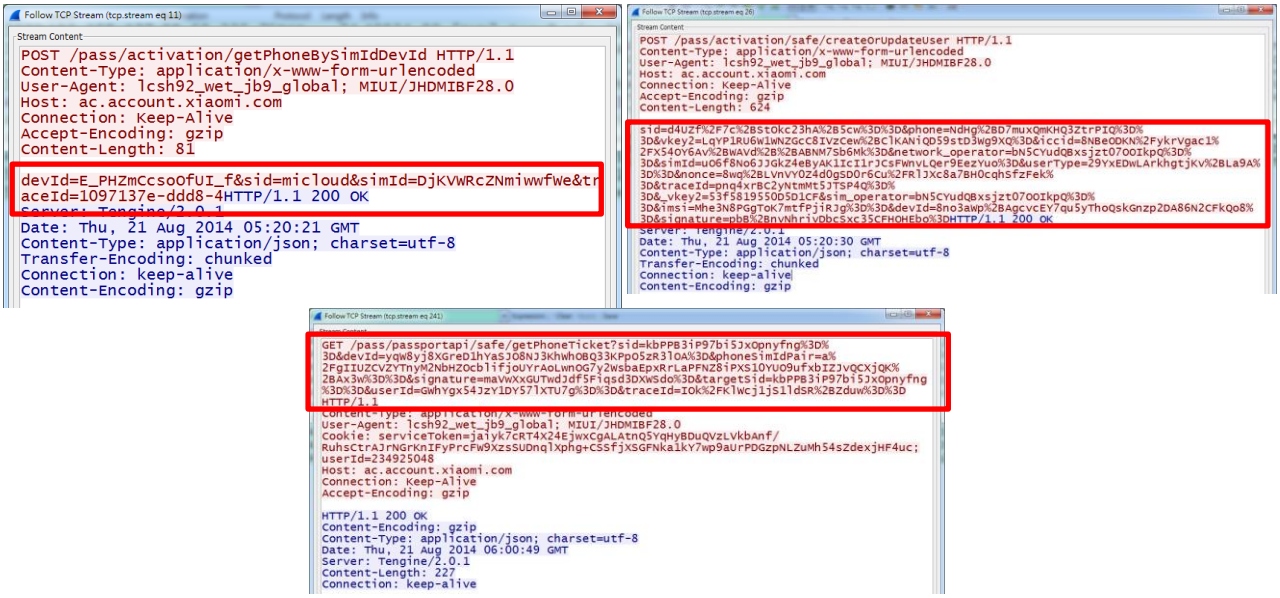
```
<bind id="X7J5D-6" to="xiaomi.com" from="263899909@xiaomi.com/E_PHZmCcsoOfUI_f" chid="3">
    <token>0QxjFrjieRMkJ7AH4gTZJOPl6pa11tOBaKat02akDkMQnKD5NsJC7IUkXNlfPL+2zINNOBrvuL66aa7gWp2Vmf9Z5k6r2QDCFE1hojwCk5qRZ+nwPQhHMR55ZJtBYDoq</token>
    <kick>0</kick><sig>bZpIFbn7M91NtoUqMOP8zbkgBUg=</sig>
    <method>XIAOMI-PASS</method>
    <client_attrs>cap:sms#mms</client_attrs>
    <cloud_attrs>phone:+88693[redacted]5 v:1</cloud_attrs>
</bind>

<bind from='xiaomi.com' to='263899909@xiaomi.com/E_PHZmCcsoOfUI_f' id='X7J5D-6' type='result' chid='3'/>
```

圖十二：XML 封包傳送本機的電話號碼至指定伺服器



圖十三：發簡訊時所傳送的封包資料



圖十四：疑似傳送裝置資訊封包圖(左上為順序 4；右上為順序 6；下為順序 15)

6. 結論

在本文中，我們介紹三個組織所提及到手機安全風險，並將其分類成伺服器因素、程式因素、傳輸因素以及人為因素共四大類。接者我們利用三種方式來測試手機的安全性，包括特徵碼掃描、權限瀏覽以及網路行為分析。特徵碼掃描是最快能找出是否藏有惡意程式或是病毒的方法，但若特徵碼採用隱藏或是分散方式將不容易發現，導致無法偵測出有異常。權限瀏覽可以發現有越權的應用程式，可以達到減少分析應用程式的數量。網路行為分析是利用封包分析來確認手機是否有傳輸個人資料到指定伺服器上，雖然可以看到所有應用程式利用 Wi-Fi 所傳輸的封包，但若應用程式指定只能利用行動網路傳輸資料，又或者是可能將資料利用加密方法轉為密文或是利用加密方式來進行傳輸，會造成此分析方法無法分析出可疑的網路行為。

最後，我們利用所提出的測試方法進行測試紅米 Note 以及 S3，兩支手機各分別有一個應用程式偵測到異常；紅米 Note 在 128 個內建應用程式中，含有 34 個疑似越權的應用程式，S3 則在 210 個內建應用程式中，含有 63 個疑似越權的應用程式；S3 在網路行為中，未發現傳輸個人資料在其中，紅米 Note 則是有發現傳輸本機手機號碼、IMEI、應用程式清單、接收簡訊的手機號碼等至特定伺服器。此外，我們也發現紅米 Note 利用亂碼方式傳輸疑似裝置資訊到特定伺服器中。

7. 參考文獻

[1] 黃彥棻," 小米手機偷傳資料到北京？iThome 找資安專家實測：有,"
http://www.ithome.com.tw/news/89991

[2] " ANDROID SMARTPHONE SHIPPED WITH SPYWARE,"
https://www.gdatasoftware.com/newsroom/news/article/android-smartphone-shipped-with-spyware.html

[3] Forristal , Jeff." Android Fake ID Vulnerability Lets Malware Impersonate Trusted Applications, Puts All Android Users Since January 2010 At Risk,"

[4] 王靖怡," NCC：明年底建立手機資安認證,"
http://www.cna.com.tw/news/aedu/201408130401-1.aspx

[5] " OWASP Mobile Security Project,"
https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

[6] " Top Ten Smartphone Risks — ENISA,"
https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone- security-1/top-ten-risks

[7] " Smartphones: Information security risks, opportunities and recommendations for users,"
ENISA, Heraklion, Greece, Dec. 2010.

[8] " NetSafe Smartphone Security Report 2014,"
http://smartphones.netsafe.org.nz/Smartphone-Security-Report-2014.pdf

[9] Forristal , Jeff. " Android Master Key Exploit – Uncovering Android Master Key That Makes 99% of Devices Vulnerable," https://bluebox.com/technical/uncovering-android-master-key-that-makes-99-of-devices-vulnerable/

[10] " 安卓安全小分队发现 Android 新漏洞,"
http://blog.sina.com.cn/s/blog_be6dacae0101bksm.html

[11] " Dr.Web v.7 Anti-virus Light," https://play.google.com/store/apps/details?id=com.drweb

[12] " Malwarebytes Anti-Malware,"
https://play.google.com/store/apps/details?id=org.malwarebytes.antimalware

[13] " VirusTotal - Free Online Virus, Malware and URL Scanner,"
https://www.virustotal.com/en/

[14] " Permission Explorer,"
https://play.google.com/store/apps/details?id=com.carlocriniti.android.permission_explorer

[15] "Wireshark · Go Deep.," https://www.wireshark.org/

附錄一：紅米 Note 權限瀏覽結果報告表

Android 動態桌布 com.android.wallpaper	ACCESS_COARSE_LOCATION CAMERA	電子郵件 com.android.email	DOWNLOAD_WITHOUT_NOTIFICATION
電話 com.android.phone	ACCESS_COARSE_LOCATION DEVICE_POWER GET_ACCOUNTS REBOOT	通訊錄與撥號 com.android.contacts	ACCESS_COARSE_LOCATION ACCESS_FINE_LOCATION MANAGE_ACCOUNTS MODIFY_PHONE_STATE REBOOT
下載管理員 com.android.providers.downloads	GET_ACCOUNTS WRITE_SECURE_SETTINGS	Google Play 商店 com.android.vending	SEND_SMS SEND_SMS_NO_CONFIRMATION WRITE_SECURE_SETTINGS
主題風格 com.android.thememanager	REBOOT	錄音機 com.android.soundrecorder	GET_ACCOUNTS
系統更新 com.android.updater	ACCESS_COARSE_LOCATION	檔案管理 com.android.fileexplorer	GET_ACCOUNTS MANAGE_ACCOUNTS
相機 com.android.camera	GET_ACCOUNTS READ_SMS	瀏覽器 com.android.browser	MANAGE_ACCOUNTS READ_LOGS
時鐘 com.android.deskclock	DEVICE_POWER WRITE_SECURE_SETTINGS	設定 com.android.setting	CALL_PHONE
簡訊 com.android.mms	ACCESS_COARSE_LOCATION GET_ACCOUNTS MANAGE_ACCOUNTS READ_LOGS WRITE_SECURE_SETTINGS	Google Play 服務 com.google.android.gms	CALL_PHONE CALL_PRIVILEGED CAMERA READ_SMS RECEIVE_SMS
藍牙分享 com.android.bluetooth	CALL_PHONE CALL_PRIVILEGED MODIFY_PHONE_STATE	日曆 com.android.calendar	MANAGE_ACCOUNTS READ_CONTACTS WRITE_SECURE_SETTINGS
下載 com.android.providers.downloads.ui	WRITE_SECURE_SETTINGS	日曆儲存空間 com.android.providers.calendar	MANAGE_ACCOUNTS
聯絡人儲存空間 com.android.providers.contacts	ACCESS_COARSE_LOCATION ACCESS_FINE_LOCATION	設定精靈 com.google.android.setupwizard	CALL_PHONE
藍牙 com.mediatek.bluetooth	READ_SMS SEND_SMS WRITE_APN_SETTINGS WRITE_SMS	小米服務框架 com.xiaomi.xmsf	CALL_PHONE SEND_SMS SEND_SMS_NO_CONFIRMATION
生活黃頁 com.miui.yellowpage	SEND_SMS	網路助手 com.miui.networkassistant	RECEIVE_SMS SEND_SMS
天氣 com.miui.weather2	CALL_PHONE GET_ACCOUNTS MANAGE_ACCOUNTS READ_CONTACTS WRITE_SECURE_SETTINGS	音樂 com.miui.player	CAMERA DOWNLOAD_WITHOUT_NOTIFICATION GET_ACCOUNTS MANAGE_ACCOUNTS READ_SMS RECORD_AUDIO
小米同步 com.miui.cloudservice	GET_ACCOUNTS SEND_SMS WRITE_SECURE_SETTINGS	相簿 com.miui.gallery	ACCESS_FINE_LOCATION DEVICE_POWER MANAGE_ACCOUNTS READ_CONTACTS
系統桌面 com.miui.home	CALL_PHONE READ_CONTACTS RECORD_AUDIO	便條 com.miui.notes	GET_ACCOUNTS MANAGE_ACCOUNTS WRITE_SECURE_SETTINGS
影片播放器 com.miui.videoplayer	READ_SMS	com.cleanmaster.sdk	READ_LOGS

附錄二：S3 權限瀏覽結果報告表

聯絡人 com.android.contacts	ACCESS_COARSE_LOCATION ACCESS_FINE_LOCATION MANAGE_ACCOUNTS MODIFY_PHONE_STATE REBOOT RECORD_AUDIO	電子郵件 com.android.email	ACCESS_COARSE_LOCATION ACCESS_FINE_LOCATION READ_SMS RECEIVE_SMS SEND_SMS WRITE_SECURE_SETTINGS
聯絡人儲存區 com.android.providers.contacts	ACCESS_COARSE_LOCATION ACCESS_FINE_LOCATION	標籤 com.android.apps.tag	CALL_PHONE WRITE_SECURE_SETTINGS
設定 com.android.settings	CALL_PHONE	S Planner com.android.calendar	READ_CONTACTS READ_SMS
訊息 com.android.mms	ACCESS_FINE_LOCATION WRITE_APN_SETTINGS WRITE_CONTACTS	電話 com.android.phone	ACCESS_COARSE_LOCATION DEVICE_POWER REBOOT WRITE_SECURE_SETTINGS
撥號儲存空間 com.android.providers.telephony	READ_SMS WRITE_SMS	藍牙共享 com.android.bluetooth	WRITE_CONTACTS
Google Play 商店 com.android.vending	SEND_SMS SEND_SMS_NO_CONFIRMATION WRITE_SECURE_SETTINGS	Exchange 服務 com.android.exchange	RECEIVE_SMS SEND_SMS WRITE_SECURE_SETTINGS
網際網路 com.android.browser	DEVICE_POWER MANAGE_ACCOUNTS READ_CONTACTS READ_PROFILE	手機追蹤系統 com.android.setting.mt	READ_CONTACTS RECEIVE_SMS SEND_SMS WRITE_CONTACTS WRITE_SECURE_SETTINGS
媒體儲存空間 com.android.providers.media	READ_CONTACTS WRITE_CONTACTS	MTP 應用程式 com.android.MtpApplication	WRITE_APN_SETTINGS
Google 帳戶管理員 com.google.android.gsf.login	CALL_PHONE	S Memo com.google.android.widgetapp.diotek.smemo	GET_ACCOUNTS READ_SMS WRITE_SMS
Google 服務架構 com.google.android.gsf	CALL_PHONE WRITE_SECURE_SETTINGS	設定精靈 com.google.android.setupwizard	CALL_PHONE
Google Partner Setup com.google.android.partnersetup	GET_ACCOUNTS	Talk com.google.android.talk	WRITE_CONTACTS
Google Play 服務 com.google.android.gms	CALL_PHONE CALL_PRIVILEGED CAMERA READ_SMS RECEIVE_SMS RECORD_AUDIO	Google 搜尋 com.google.android.googlequicksearchbox	CALL_PHONE MANAGE_ACCOUNTS READ_SMS SEND_SMS WRITE_SECURE_SETTINGS WRITE_SMS
DSMLawmo com.sec.dsm.system	READ_SMS RECEIVE_SMS WRITE_SMS	DttSupport com.sec.android.dttsupport	CAMERA READ_SMS WRITE_SMS
SecSetupWizard com.sec.android.app.SecSetupWizard	CALL_PHONE READ_CONTACTS	SNS com.sec.android.app.sns3	GET_ACCOUNTS MANAGE_ACCOUNTS
音樂播放器 com.sec.android.app.music	READ_SMS RECORD_AUDIO	相機 com.sec.android.app.camera	READ_SMS WRITE_SECURE_SETTINGS
PhoneUtil com.sec.android.app.phoneutil	DEVICE_POWER MODIFY_PHONE_STATE	錯誤 com.sec.app.RilErrorNotifier	CALL_PHONE WRITE_APN_SETTINGS
ChatON com.sec.chaton	CALL_PHONE READ_LOGS RECEIVE_SMS WRITE_CONTACTS	Samsung Apps com.sec.android.app.samsungapps	CALL_PHONE RECEIVE_SMS SEND_SMS WRITE_APN_SETTINGS
FM 收音機 com.sec.android.app.fm	CALL_PHONE	SamsungAppsUNA2 com.sec.android.app.samsungapps.una2	CAMERA
LogsProvider com.sec.android.provider.logsprovider	WRITE_CONTACTS	三星鍵盤 com.sec.android.inputmethod	READ_SMS
SASlideShow com.sec.android.saslideshow	ACCESS_COARSE_LOCATION ACCESS_FINE_LOCATION GET_ACCOUNTS MANAGE_ACCOUNTS READ_CONTACTS READ_PROFILE READ_SMS	媒體瀏覽器 com.sec.android.gallery3d	ACCESS_COARSE_LOCATION ACCESS_FINE_LOCATION CALL_PRIVILEGED GET_ACCOUNTS MANAGE_ACCOUNTS READ_CONTACTS READ_PROFILE READ_SMS RECORD_AUDIO

影片播放器 com.sec.android.app.videoplayer	ACCESS_FINE_LOCATION READ_SMS RECEIVE_SMS RECORD_AUDIO WRITE_SMS	CSC com.samsung.sec.android.application.csc	ACCESS_FINE_LOCATION READ_CONTACTS WRITE_CONTACTS WRITE_SECURE_SETTINGS
Weather Widget com.sec.android.widgetapp.ap.hero.accuweather.widget	READ_CONTACTS READ_PROFILE	Weather Widget Main com.sec.android.widgetapp.ap.hero.accuweather	READ_CONTACTS
AllShare Service com.sec.android.allshare.framework	READ_SMS	時鐘 com.sec.android.app.clockpackage	RECORD_AUDIO
Samsung Cloud Data Relay com.sec.android.sCloudRelayData	WRITE_SECURE_SETTINGS	雙時鐘(數位式) com.sec.android.widgetapp.dualclockdigital	WRITE_SECURE_SETTINGS
Samsung Syncadapters com.sec.android.sCloudSync	WRITE_SECURE_SETTINGS	雙時鐘(類比式) com.sec.android.widgetapp.dualclockanalog	WRITE_SECURE_SETTINGS
Samsung Backup com.sec.android.sCloudBackupApp	WRITE_SMS	Samsung Backup Provider com.sec.android.sCloudBackupProvider	WRITE_SMS
DataCreate com.sec.android.app.DataCreate	WRITE_SMS	風向天氣 com.sec.ccl.csp.app.secretwallpaper.themetwo	WRITE_SECURE_SETTINGS
AllShare Play com.sec.pcw	READ_CONTACTS	SyncmlDS com.smlds	GET_ACCOUNTS
Polaris Viewer4.1 com.infraware.polarisviewer4	CALL_PHONE GET_ACCOUNTS MANAGE_ACCOUNTS SEND_SMS WRITE_CONTACTS	軟體更新 com.wssyncmldm	CALL_PHONE GET_ACCOUNTS RECEIVE_SMS SEND_SMS WRITE_SMS
MAPServiceSamsung com.samsung.map	READ_CONTACTS READ_SMS RECEIVE_SMS SEND_SMS WRITE_SMS	joyn com.samsung.rcs	WRITE_APN_SETTINGS WRITE_CONTACTS WRITE_SECURE_SETTINGS WRITE_SMS
S Suggest com.tgrape.android.radar	REBOOT	三星帳號 com.osp.app.signin	WRITE_APN_SETTINGS
wssyncmlnps com.wssnps	GET_ACCOUNTS READ_SMS RECEIVE_SMS SEND_SMS WRITE_CONTACTS WRITE_SMS		