Research Center for information Technology Innovation
TWISC
TAIWAN INFORMATION SECURITY CENTER

中央研究院-資通安全研究與教育中心

資安前瞻關鍵技術基礎研究計畫

智慧型手機資安檢測報告

Smart Phone Security Test Report

前瞻議題研究小組 張宏昌 博士

TWISC
Taiwan Information Security Center

一、研究背景及目的

大陸手機近期遭質疑有資安疑慮，引起外界極大話題。國家通訊傳播委員會(NCC)對此議題表示，目前電信基地台因國安因素禁用陸製設備之外，手機則有「資安檢測(ESS)」，但沒有強制性，市面上多數手機都沒有經過檢測。目前國內手機資安檢測採業者自願送測的模式，並不像手機型式認證，強制要求廠商在台灣販售必須送審，所以無從得知是否有產品送測未通過。事實上，NCC 所推出的資安檢測，分為初、中、高級，初級規範如蒐集個人隱私敏感性資料前，必須明確告知使用者；中級則要求手機應提供完整資料保護機制，包含資料在使用、儲存及傳輸時，皆可獲得安全保護；高級必須做到確保手機核心底層不被竄改或被不正當的獲取資訊。

針對美、英、日、澳、紐等國家，都禁用華為手機，現在也傳出政府要求國銀業者，基於資安考量跟進禁用大陸產品，包括手機、通訊軟體等，尤其公股銀行董事長、總經理等重要人員，如此表示行動產品的資安檢測代表著未來行動資安的重要趨勢。藉由對智慧型手機行動裝置資通安全檢測，提出資安檢測報告，提供給相關單位參考，並可加強民眾個資及隱私防護之認知。

二、基礎檢測項目及內容

本報告依據智慧型手機系統內建軟體資安檢測，針對不同面向之行動應用程式安全來訂定基本資安檢測項目，其中包括 [檢測手機開機後之網路行為]、[檢測手機啟動各項服務後之網路行為]、[內建軟體原始碼反組譯及權限分析]、[檢測資料傳輸及儲存安全五大項目] 等四大項目，針對每一檢測項目，技術要求、檢測基準及檢測結果等欄位並說明如表 1 所示。其中針對手機內的資料是否涉及敏感資料及是否為使用者輸入之隱私資料等，如表 2 所示，會將於測試中將之分類及檢測。

表 1 檢測項目及內容表

檢測項目	檢測內容
1.檢測手機開機後之網路行為	1.1 手機無 SIM 卡，僅由 WiFi 連結網路，如未傳輸第 1 類明文資料，或傳輸加密資料，或傳輸第 1 類(除帳號、密碼或通訊錄內容外)明文資料前，已取得使用者同意。
	1.2 手機有 SIM 卡，僅由 WiFi 連結網路，如未傳輸第 1 類明文資料，或傳輸加密資料，或傳輸第 1 類(除帳號、密碼或通訊錄內容外)明文資料前，已取得使用者同意。
	1.3 手機有 SIM 卡，僅由行動網路連結網路，如未傳輸第 1 類明文資料，或傳輸加密資料，或傳輸第 1 類(除帳號、密碼或通訊錄內容外)明文資料前，已取得使用者同意。
2.檢測手機啟動各項服務後之網路行為	2.1 手機有 SIM 卡，僅由 WiFi 連結網路，如未傳輸第 1 類明文資料，或傳輸加密資料，或傳輸第 1 類(除帳號、密碼或通訊錄內容外)明文資料前，已取得使用者同意。
	2.2 手機有 SIM 卡，僅由行動網路連結網路，如未傳輸第 1 類明文資料，或傳輸加密資料，或傳輸第 1 類(除帳號、密碼或通訊錄內容外)明文資料前，已取得使用者同意。

3.內建軟體原始碼反組譯及權限分析	3.1 利用自行開發之手機 APP 逆向原始碼分析平台反組譯及權限分析，取得非法權限之宣告及權限開啟。	
4.檢測資料傳輸及儲存安全	4.1 資料傳輸安全：各內建軟體如帳號、密碼或通訊錄內容資料加密，或使用加密傳輸通道。	5.1.1 手機有 SIM 卡，僅由 WiFi 連結網路
		5.1.2 手機有 SIM 卡，僅由行動網路連結網路
	5.2 資料儲存安全：各內建軟體於儲存帳號、密碼或通訊錄內容資料時，使用加密方式儲存，或儲存於手機作業系統限制存取之區域。	

表 2 資料內容分類表

類別	資料內容	是否涉及敏感資料	是否為使用者輸入
第 1 類	帳號密碼、聯絡方式(通訊錄，如：姓名、地址、電話、電子郵件等包含但不限於之相關資訊)、簡訊內容、通話錄音、個人影音或個人文件檔	是	是
第 2 類	IMEI、IMSI 或定位資訊	是	否
第 3 類	App 列表、音樂撥放資訊、手機作業系統、手機型號、手機韌體版本、MCC、MNC、行動通信業者或網路傳送方式	否	否
第 4 類	資料加密、協定加密或無加密但內容未知	N/A	N/A

三、待測之智慧型手機

此次待測之手機選擇如表 3 所示，選擇近期台灣較熱門流行及具代表性之手機，中國手機有華為、小米、OPPO 三款，韓國 LG 一款，台灣 HTC 一款，共計五款手機待測。

表 3 待測之智慧型手機列表

手機	 OPPO R11s Plus	 Xiaomi MIX 2S	 HUAWEI P20 Pro	 LG G5	 HTC One M9+
上市時間	2017-12-22	2018-05-09	2018-04-25	2016-04-12	2015-05-15
國家	中國	中國	中國	韓國	台灣

四、智慧型手機系統內建軟體資通安全檢測等級

為配合不同安全需求，將智慧型手機系統內建軟體資通安全等級區分為初級、中級及高級 3 種，各等級之要求及說明如表 4。

表 4　資通安全等級之要求及說明

資通安全等級	要求	說明
初級 (B)	智慧型手機應提供個人隱私相關的資料安全，包含手機安全性功能和敏感性資料相關保護，如蒐集敏感性資料的行為必須明確告知使用者。	為智慧型手機基本隱私保護之最低要求。
中級 (M)	智慧型手機應提供完整資料保護機制，包含所有資料在使用、儲存及傳輸時，皆可被安全保護。	除須符合初級之所有必測細項外，並增加資料進階保護之檢測細項。
高級 (H)	智慧型手機應確保核心底層不被竄改或被不正當的擷取資訊。	為確保智慧型手機之核心底層不會被竄改或不正當地擷取資訊，除須符合初級與中級之所有必測細項外，並增加手機設計相關安全性文件審查之檢測細項。

五、檢測流程方法

本測試報告主要是針對實體手機本身內建應用程式進行監控，將過往筆者研究中所得出的惡意程式特徵結果統整提出一套檢測方法使用在 Android 實體手機上。首先將實體手機還原為原廠設定進行檢測，在靜態分析中將手機內部應用程式取出來做特徵碼掃描以及權限分析，在動態分析中檢測手機內部應用程式的使用狀況 CPU、RAM、Logcat 訊息、網路封包，將取得結果與惡意程式的特徵進行分析是否有安全疑慮，圖 1 為手機測試系統架構。

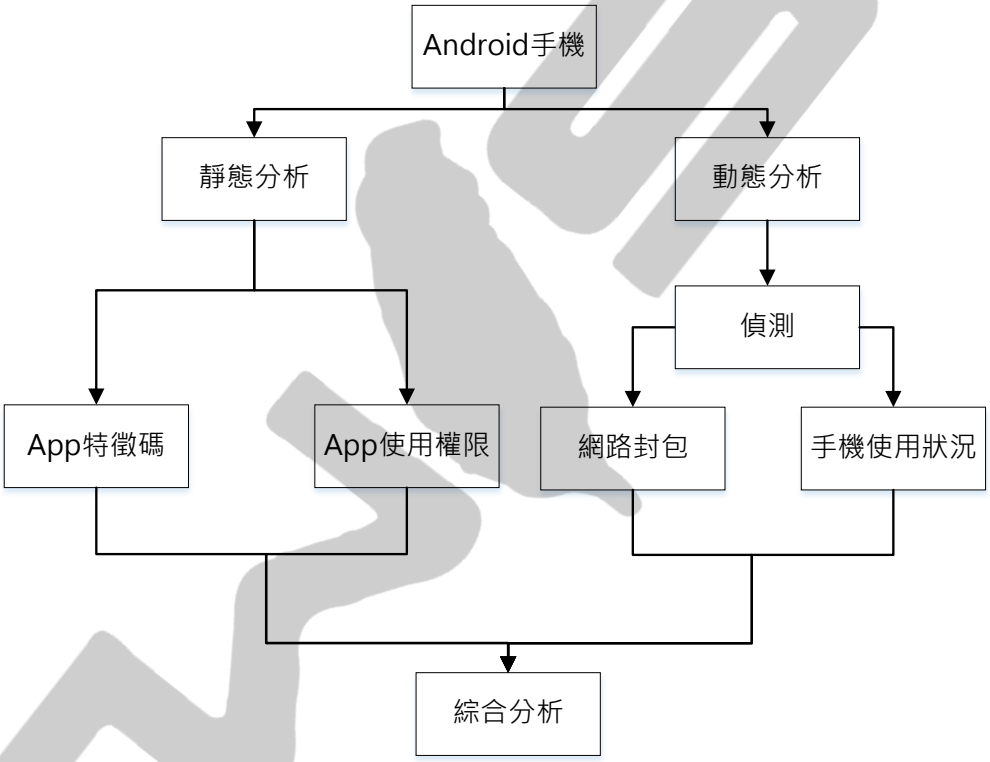

圖 1 手機測試系統架構

目前手機動態分析工具都以虛擬機為主，而本測試報告要以實體手機作為實驗，因此使用自行開發之測試系統取得手機使用的狀態此系統為 ADB 動態。此系統主要包含

應用程式網路行為、CPU 使用狀況、RAM 的使用狀況、Logcat 訊息等。ADB 動態系統使用 Android SDK tools ADB 的指令並系統所需功能，再將手機內部資料取出儲存於.csv 格式方便後續分析使用，表 5 為此系統功能。

表 5 系統功能

功能	說明
行動裝置資訊	了解廠牌、型號、Android 版本、目前手機時間
電池	了解目前手機電池電量、溫度
基本資料	了解手機韌體版本、裝置機板代號等資訊
儲存空間資訊	了解手機目前資料夾使用容量
網路介面	了解目前手機內部 Wi-Fi、p2p 等網路介面
網路連線	了解目前手機應用程式使用網路狀態、IP
CPU 狀態	了解目前手機 CPU 頻率、CPU 溫度
CPU 使用資訊	了解目前手機系統使用狀況
RAM 使用資訊	了解目前手機記憶體使用狀況
程序使用資訊	了解目前手機 CPU 使用狀況
LOG 訊息	了解目前手機調用狀況

使用上述表 5 的功能我們需要使用 ADB 工具讓手機與系統溝通，並且在系統中互相調用資料，例如網路連線使用 ADB 命令可以得知網路使用狀況，但無法得知是哪

個應用程式所使用的必須再搭配其他 ADB 命令，因此本系統使用多個 ADB 命令，表 6 列出幾個系統較為重要的命令。

表 6　ADB 指令說明

指令	功能
adb shell dumpsys package p	手機應用程式的 UID 碼
adb shell dumpsys battery	手機電池的使用狀況
adb shell dumpsys meminfo	手機應用程式使用的記憶體的狀況
adb shell df	手機資料夾使用狀況
adb shell getprop	手機硬體、廠商、IMEI 等資訊
adb shell logcat	手機調用資訊及狀況
adb shell netcfg	手機網路使用狀況
adb shell top	手機 CPU 使用狀況

六、檢測結果

(1)手機連線至各國伺服器情況

如圖 2 所示，依下列三種測試情境，利用以下動態分析檢測流程來檢測手機連線至各國伺服器情況，說明如下:

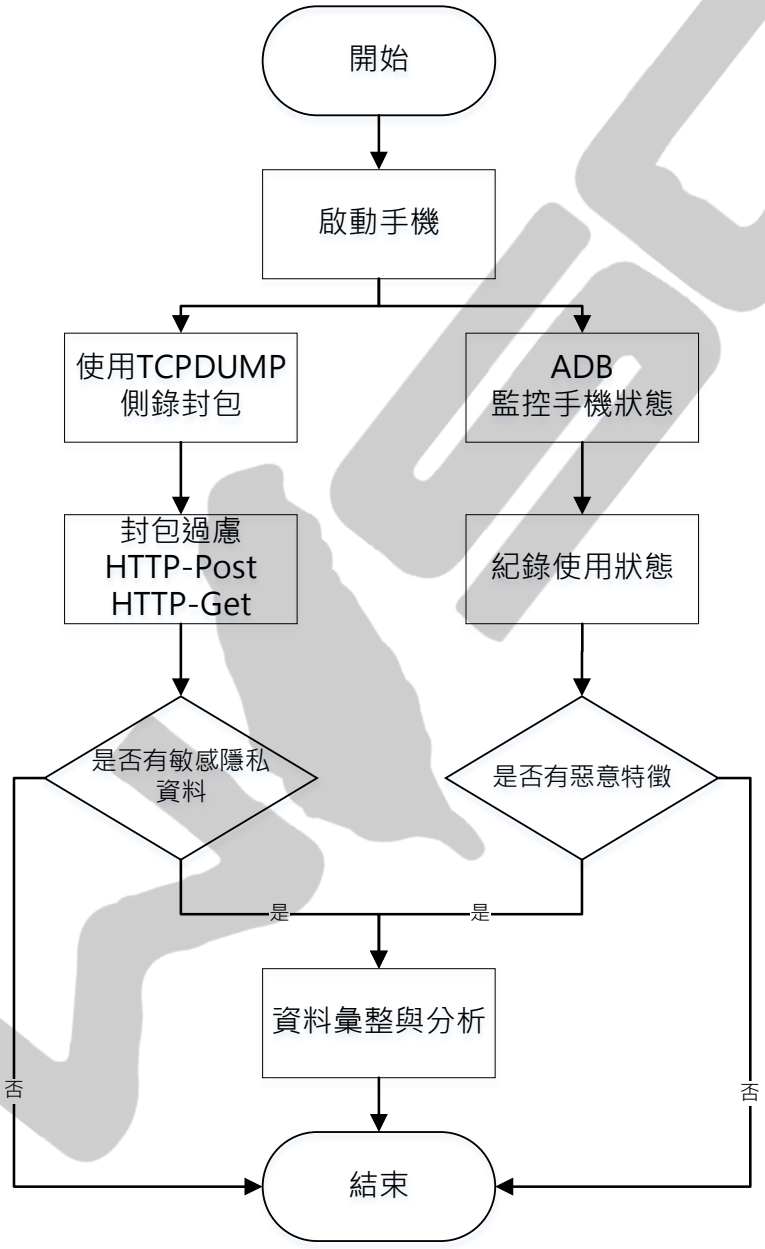

圖 2　動態分析流程

- 無 SIM 卡手機開機時，以 WiFi 上網，各手機連接至各國伺服器情況

所有手機於開機時，皆會與亞洲的伺服器連線，如圖 3　OPPO R11s Plus 手機

連網狀況所示，手機開機後即會連回新加坡伺服器；尤其 3 款中國研發生產連線流量較多，推測應是進行系統或者使用者資料回傳及更新作業。然而手機廠商與連線伺服器所在國家似無明顯關聯性。

- 有 SIM 卡手機開機時，以 WiFi 上網，各手機連接至各國伺服器情況

  所有手機於開機時，皆會與亞洲的伺服器連線。連線國家數量較多的為網路校時行為。然而手機廠商與連線伺服器所在國家仍無明顯關聯性。

- 有 SIM 卡手機開機時，以行動網路上網，各手機連接至各國　　伺服器情況

  分析 5 款手機有 SIM 卡開機時，以行動網路上網連線國家情況，其中所有手機於開機時，仍皆會與亞洲的伺服器連線。然而手機廠商與連線伺服器所在國家仍無明顯關聯性。

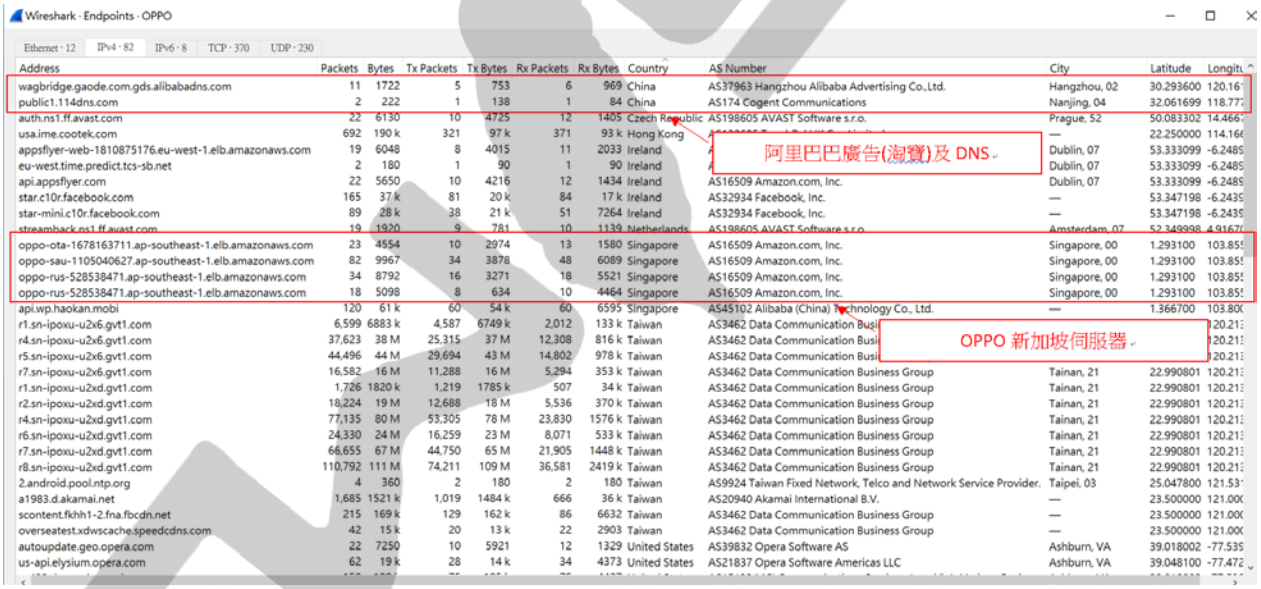

圖 3　OPPO R11s Plus 手機連網狀況

(2) 各手機背景傳送資料情況

依下列三種測試情境，檢測各手機背景傳送資料情況，說明如下:

- 無 SIM 卡手機開機時，以 WiFi 上網，各手機背景傳送資料情況
- 有 SIM 卡手機開機時，以 WiFi 上網，各手機背景傳送資料情況
- 有 SIM 卡手機開機時，以行動網路上網，各手機背景傳送資料情況

以上三種測試情境傳送資料之結果，基本上針對封包分析結果，皆有回傳手機基本資訊如 IMEI、MSI、GPS 定位、手機作業系統、手機型號、手機韌體版本、MCC、MNC 等，應為手機原廠確認更新資訊及登錄使用者資料等行為。

但是在大陸品牌手機方面，如圖 4 所示，發現 OPPO R11s Plus 手機連網時在未加密狀況下會傳送系統相關機密設定訊息及系統資訊回新加坡伺服器，其中 OPPO R11s Plus 手機回傳之封包內容利用 Pcap Analyzer 系統分析，內容中甚至檢測出包含未加密的 SQL 注入攻擊危險之指令，如圖 5 所示，封包包含 SQL 注入攻擊危險之指令字串，代表在 OPPO 通訊開發安全部分還潛在著機訊資訊未加密及 SQL INJECTION 等漏洞。其它 2 款中國手機因傳輸封包都加密，無法得知回傳之內容，傳輸之封包經資安軟體檢測都沒有危險性攻擊之異常訊息指令。

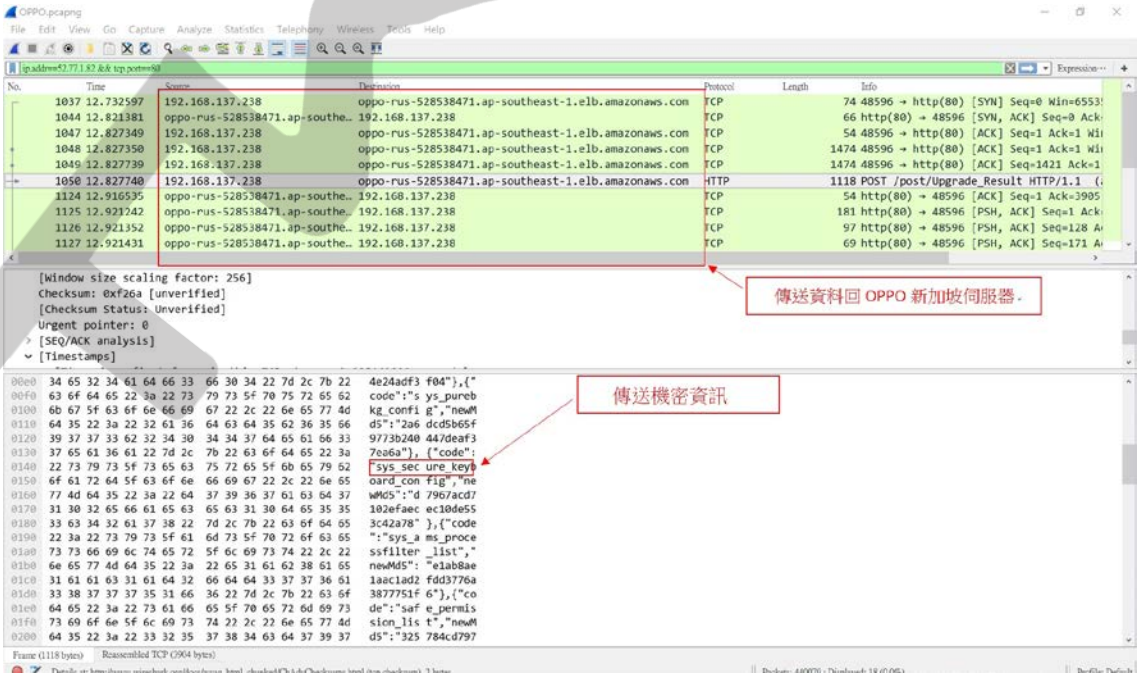

圖 4 OPPO R11s Plus 未加密狀況下會傳送機密設定訊息

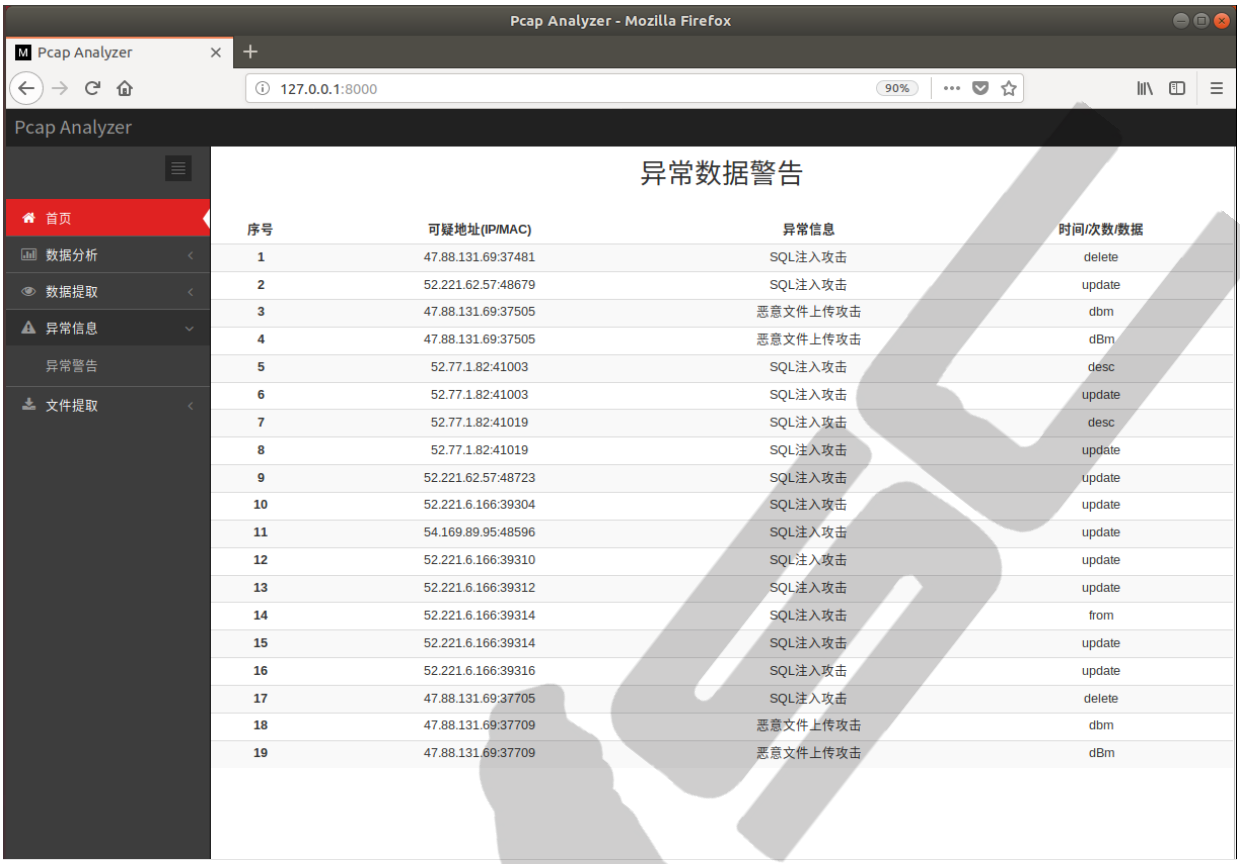

圖 5 OPPO R11s Plus 回傳包含 SQL 注入攻擊危險之指令

在網路行為分析中待測之 5 款手機的結果都不一樣，我們將手機內部應用程式全數監控網路傳輸內容，表 7 可以發現每台手機基本上都會傳輸 IMEI、手機作業系統、手機型號、MCC、MNC，其中又以大陸 3 款手機傳輸的內容較多，甚至有使用輸入之隱私資料及未知加密資料等。

表 7 各廠牌手機傳輸資料內容表

手機廠牌	OPPO R11s Plus	Xiaomi MIX 2S	HUAWEI P20 Pro	LG G5	HTC One M9+
IMEI	✓	✓	✓	✓	✓
IMSI	✓	✓	✓		
GPS 定位	✓	✓	✓	✓	✓
手機作業系統	✓	✓	✓	✓	✓
手機型號	✓	✓	✓	✓	✓
手機韌體版本	✓	✓	✓	✓	✓
MCC	✓	✓	✓	✓	✓
MNC	✓	✓	✓	✓	✓
書籤內容		✓			
手機設定	✓	✓	✓		
自動下載檔案	✓	✓	✓		
資料加密，內容未知	✓	✓	✓		

(4) 原生系統軟體檢測

原生系統軟體檢測流程使用 google Virustotal 檢測及自行開發之手機 APP 逆向原始碼分析平台等工具來反組譯及權限分析，取得非法權限之宣告及權限開啟。如下表及圖三所示，中國研發製造之 OPPO R11s Plus、Xiaomi MIX 2S、HUAWEI P20 Pro 手機皆檢測出惡意程式。

除了上傳 Virustotal 檢查外，原生程式自我權限分析要判別應用程式(APP)是否有安全疑慮問題，更是重要的檢查項目，因此我們將先前有關惡意程式權限分析的研究選出幾個可能造成手機安全疑慮的權限，再加上此研究主要了解是否有手機本身將個人資料外洩的疑慮，多加了可讀取手機 LOG 權限(如 READ_CALL_LOG、READ_LOG)進行分析。表 8 為此研究所列出來有安全疑慮的權限。

表 8 權限瀏覽

權限名稱	權限功能
ACCESS_COARSE_LOCATION	允許程式存取 Wi-Fi 網路狀態訊息
ACCESS_FINE_LOCATION	允許程式存取精確位置(如 GPS)
CALL_PHONE	允許一個程式初始化一個電話撥號不需透過撥號使用者界面需要使用者確認
CALL_PRIVILEGED	允許一個程式初始化一個電話撥號不需透過撥號使用者界面需要使用者確認

CAMERA	允許存取使用照相裝置
DEVICE_POWER	允許程式開啟或關閉手機
DOWNLOAD_WITHOUT_NOTIFICATION	允許程式可不告知使用者，自行下載東西
GET_ACCOUNTS	允許程式取得帳戶清單
INSTALL_PACKAGES	允許程式下載應用程式
MANAGE_ACCOUNTS	允許程式執行新增、移除帳戶和刪除帳戶密碼等作業
MODIFY_PHONE_STATE	允許程式控制裝置的電話功能。擁有這項權限的應用程式可在未通知您的情況下，任意切換網路、開啟或關閉手機無線電等
READ_CALL_LOG	允許程式讀取通話紀錄
READ_CONTACTS	允許程式讀取聯絡人資料，包括您與特定聯絡人通話、傳送電子郵件或使用其他通訊方式的互動頻率
READ_LOGS	允許程式讀取系統的各種記錄檔，可能包含個人或私人資訊
READ_PROFILE	允許程式讀取裝置上儲存的個人資料，例如您的姓名和聯絡資訊
READ_SMS	允許程式讀取簡訊

REBOOT	允許程式能夠重新啟動裝置
RECEIVE_SMS	允許程式接收和處理簡訊。這項設定可讓程式監控傳送至您裝置的訊息，或在您閱讀訊息前擅自刪除訊息
SEND_SMS	允許程式發送簡訊
SEND_SMS_NO_CONFIRMATION	允許在沒有使用者的允許下發出訊息
WRITE_APN_SETTINGS	允許程式變更網路設定，並攔截及檢查所有網路流量，惡意程式可能利用此功能，在您不知情的情況下監控、重新導向或修改網路封包
WRITE_CONTACTS	允許程式修改裝置儲存的聯絡人資料，包括您與個別聯絡人通話、電郵或以其他通訊方式聯絡的頻率。這項權限允許應用程式刪除聯絡人資料
WRITE_PROFILE	允許程式新增或變更裝置上儲存的個人資料，例如您的姓名和聯絡資訊。這項設定可讓應用程式識別您的身分，並可能將您的個人資料傳送給他人
WRITE_SECURE_SETTINGS	允許程式修改系統安全設定資料
WRITE_SMS	允許程式寫入裝置或 SIM 卡中儲存的短訊。

	惡意應用程式可能會藉此刪除您的訊息

靜態分析使用的工具為Google 的線上病毒檢測系統 Virustotal 以及 Android SDK tools AAPT。靜態分析流程主要先將手機回到原廠設定將手機內建應用程式取出，使用 Virustotal 檢測應用程式特徵碼是否有安全疑慮，以及使用 AAPT 進行應用程式權限掃描，再經由上述列出可能有安全疑慮的權限進行篩選，將有安全疑慮的應用程式記錄下來如圖 6 為靜態分析流程。

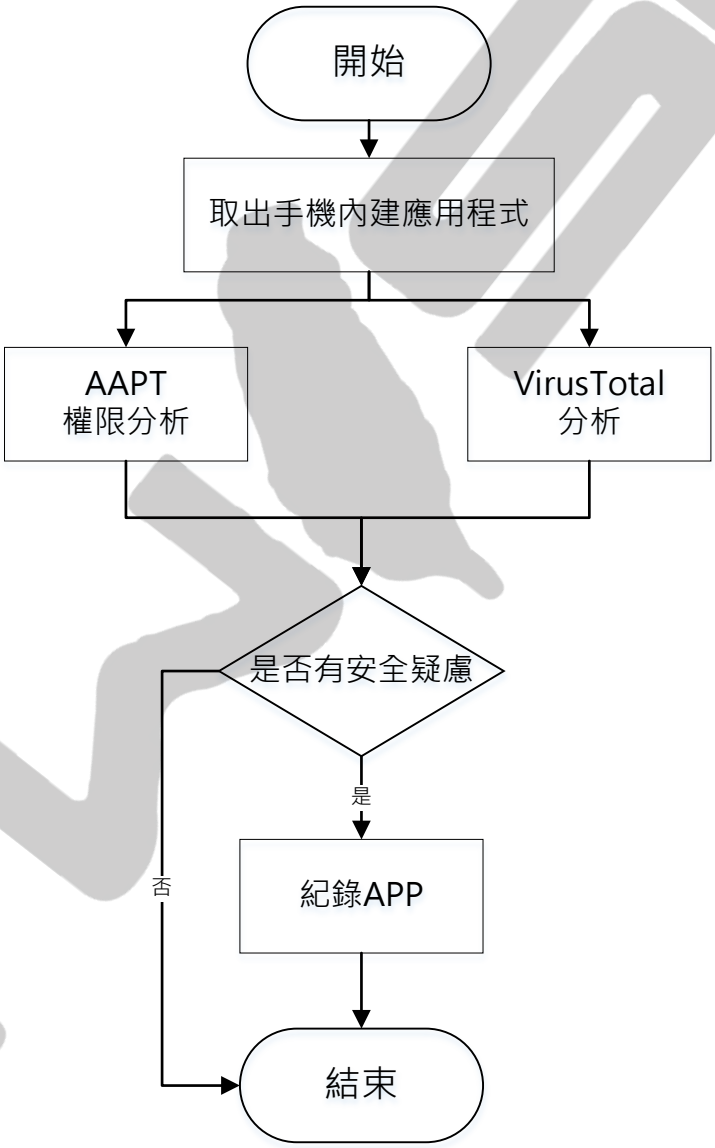

圖 6 靜態分析流程

利用 Virustotal 上傳檢測手機出廠時的原生之 APP，檢測出異常之手機原生惡意 APP，並利用自行開發之 APP 原始碼反組譯及權限分析系統，取得非法權限之宣告及權限開啟之惡意 APP 軟體，列表如下表所示，產生之結果如圖 7 所示，統計如果如表 8 所示。以 OPPO R11s Plus 手機之主題商店 APP 軟體為例，在表 10 及圖 8 中，可以看到 [6.主題商店_com.nearme.themespace.apk.txt] 在功能性上不會存取到手機的簡訊，但是系統權限上則將存取簡訊的權限全都開啟，造成資安上的風險存在。

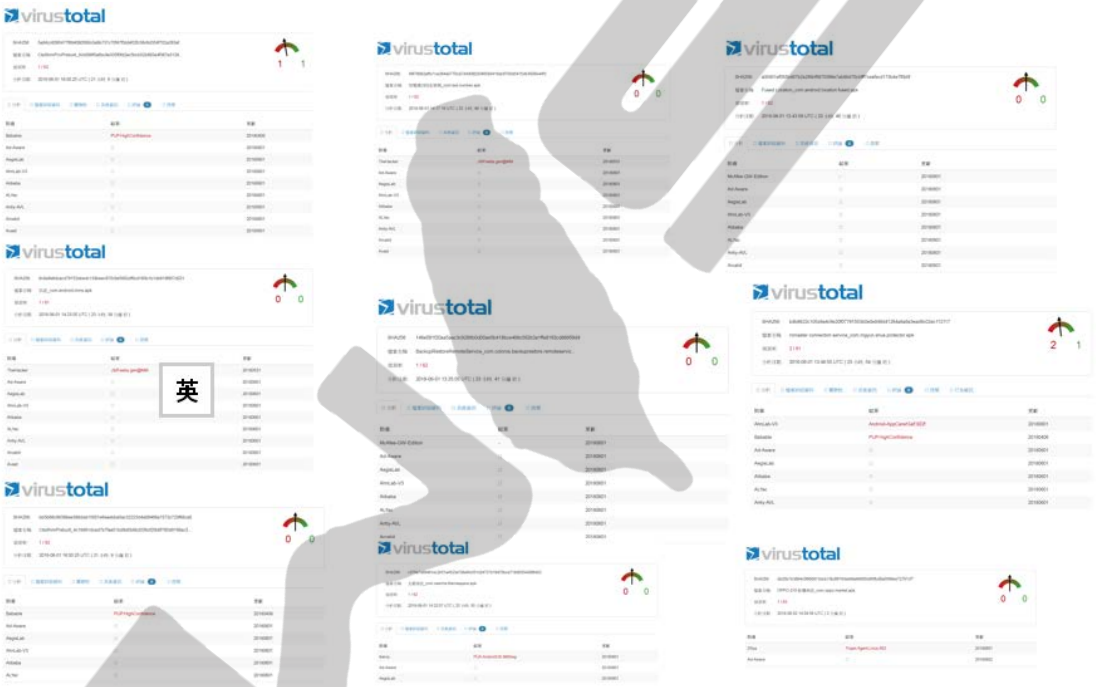

圖 7 手機原生 APP 上傳 Virustotal 檢測結果

表 9 Virustotal 手機檢測結果列表

手機	OPPO R11s Plus	Xiaomi MIX 2S	HUAWEI P20 Pro	LG G5	HTC One M9+
原生 APP	253	232	243	192	201

數量					
Virustotal 檢測異常	9	8	8	0	0

表 10 手機原生惡意 APP 軟體列表

手機	惡意 APP 軟體
OPPO R11s Plus	1. BackupRestoreRemoteService_com.coloros.backuprestore.remoteservice.apk.txt 2. com.android.cts.ctsshim_com.android.cts.ctsshim.apk.txt 3. com.android.cts.priv.ctsshim_com.android.cts.priv.ctsshim.apk.txt 4. Fused_Location_com.android.location.fused.apk.txt 5. romaster_connection_service_com.mgyun.shua.protector.apk.txt 6. 主題商店_com.nearme.themespace.apk.txt 7. 訊息_com.android.mms.apk.txt 8. 軟體商店_com.oppo.market.apk.txt 9. 智慧識別陌生號碼_com.ted.number.apk.txt
Xiaomi MIX 2S	1. com.android.cts.priv.ctsshim_com.android.cts.priv.ctsshim 2. 日曆_com.android.calendar 3. 米幣支付_com.xiaomi.payment
HUAWEI P20 Pro	4. Asphalt_Nitro_com.gameloft.android.GloftANPH.apk.txt 5. com.android.cts.ctsshim_com.android.cts.ctsshim.apk.txt 6. com.android.cts.priv.ctsshim_com.android.cts.priv.ctsshim.apk.txt 7. Google_com.google.android.googlequicksearchbox.apk.txt 8. Messenger_com.facebook.orca.apk.txt 9. TalkBack_com.google.android.marvin.talkback.apk.txt 10. 極相機_com.jb.zcamera.apk.txt 11. 運動健康_com.huawei.health.apk.txt

圖 8 自行開發手機 APP 逆向原始碼分析平台之非法權限分析

七、結論

經過一系列的檢測及分析，資通安全等級測試如表 11 所示，我們能夠發現在測試的 5 款手機中，大陸 3 款手機不論在特徵碼分析、權限分析、網路行為以及手機狀況，相較與其他韓廠、台廠牌手機有較高的危險性。不管在資料回傳及原生系統 APP 部分，都隱含了極大的資安危機及風險，再加上此 3 款手機是時下台灣及亞洲地區極流行及廠商主力推廣之手機，更是加速了資安危機的擴散程度。

本研究並沒辦法完全證明使用這些手機絕對是惡意的，只是提出實際測試數據及警示訊息，在網路行為方面有些資訊是有經過加密處理無法完全了解內部的內容，甚至有些惡意程式並需要在長時間或者特殊條件下才能觀察出來，期望未來能夠開發更完整的自動化測試系統，並針對加密封包加以分析，並長期及動態觀察系統的變化及行為偵測。

表 11　資通安全等級測試表

資通安全等級	OPPO R11s Plus	Xiaomi MIX 2S	HUAWEI P20 Pro	LG G5	HTC One M9+
初級 (B)	通過	通過	通過	通過	通過
中級 (M)	通過	通過	通過	通過	通過
高級 (H)	**回傳惡意及不明加密資訊**	**回傳不明加密之系統或使用者資訊**	**回傳不明加密之系統或使用者資訊**	回傳手機基本資訊	回傳手機基本資訊