手持行動通訊裝置之通訊安全探討－以手機竊聽軟體造成之犯罪隱憂為例

楊凱勝　蔣文棋　莊明雄
內政部警政署刑事警察局 刑事研究發展室
組長　研發役　警務正
yccs@email.cib.gov.tw　freelock@email.cib.gov.tw　saxbear@email.cib.gov.tw

摘要

隨著電子科技進步，NOKIA、HTC 等全球知名品牌大量採用開放式作業系統，不僅讓手機更具智慧，卻也埋下資通犯罪的隱形炸彈。近年來國內新聞常報導非法竊聽犯罪案件，尤以徵信業、通訊器材業等之從業人員最為猖獗，嚴重侵害人民秘密通訊自由、隱私權，造成國內民眾人心惶惶。98 年度刑事警察局破獲數起徵信業利用手機竊聽軟體進行竊聽案件，顯示大眾仍可能處於遭竊聽的不安風險中。有鑑於此，本篇文章將探討手機竊聽軟體的功能，說明防制的方法與排除作法，有效阻絕被監控的風險。

關鍵詞：手持行動通訊裝置、通訊安全、手機竊聽軟體、智慧型手機、非法竊聽

1. 前言

全錄帕羅奧圖研究中心（Palo Alto Research Center；PARC）前首席科技長馬克・懷瑟（Mark Weiser）曾於 1991 年 9 月在科學的美國人雜誌(Scientific American)發表「二十一世紀的電腦」（The Computer for 21th Century）文章，文中提出「影響最深遠的科技是消失的科技，它們已融入在我們每日的生活中，與生活密不可分。」前瞻性概念觀點[7-8]。

現今科技昌明進步，新興資通訊科技（Information Communication Technology；ICT）的發明精進，使得各式便利的 3C 消費性電子產品快速普及應用，讓人們無時無刻享受著前述以「消失」型態概念展現，但卻能隨時、隨地，即時提供便捷服務，滿足需求的新穎科技產物。1973 年由 Motorola 公司 Dr. Cooper 等人發明手持行動通訊裝置－行動電話便是一項近代的革命性科技產品[6]。

從 1973 年至今，手持行動通訊裝置的推陳出新，數位化、多元化運用，使得人們可遠距離雙向聯繫溝通更具便利性與多樣化，而其間的通訊安全則是我們持續關注的焦點。近年來國內新聞常報導非法竊聽犯罪案件，尤以徵信業、通訊器材業等之從業人員最為猖獗，嚴重侵害人民秘密通訊自由、隱私權，造成國內民眾人心惶惶。馬總統於就任之初，即多次公開宣示強力打擊非法監聽之惡行，更為杜絕非法竊聽行為組成「打擊坊間非法竊聽專案小組」，內政部警政署於 98 年 2 月 18 日頒訂「警察機關查處坊間非法竊聽執行計畫」，澈底將非法竊聽案件列為重要專案，以保障憲法賦予人民秘密通訊自由、保護隱私權等之基本權利。

98 年間刑事局陸續破獲古姓女子所經營之恆○偵防科技實業有限公司使用的手機竊聽軟體（以下簡稱竊聽軟體）「萬里通」供人竊聽案及郭○發等 8 人成立中○徵信社竊聽案[3]，顯見國內不法人士利用手機軟體進行竊聽之案件，有增加的趨勢，致大眾處於遭竊聽的不安風險中。

隨著電子科技進步，NOKIA、HTC 等全球知名品牌大量採用開放式作業系統（Operating System），加上各式各樣的手機軟體套件開發搭配，不僅讓手機更具智慧性，卻也埋下資通犯罪的隱形炸彈，未來不排除可能遭不法集團濫用手機簡訊傳遞惡意程式訊息，誘使被害人主動選取並安裝，趁機瞭解被害人的隱私狀況及掌握其日常作息，藉以進行各式犯罪，諸如詐騙、恐嚇取財等，本文將探討現行手機竊聽軟體造成之犯罪隱憂問題，並進一步提供解析之道。

2. 智慧型手機的介紹與犯罪隱憂

「智慧型手機」（Smart Phone）即手機結合個人電腦相關功能，匯集多媒體展示、無線

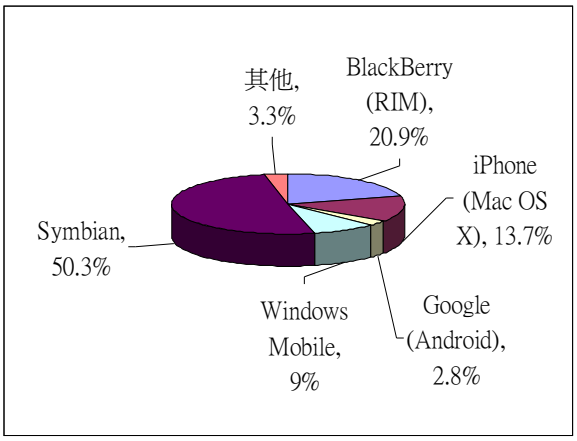

圖 1 2009 年第二季全球手機開放式系統市占率

網路傳輸、中央處理器速度快等優勢，並採用開放式作業系統，讓第三方（Third Party）業者可以開發相關的應用軟體，便利用戶自行安裝所需的軟體程式，目前開放式系統包括：Symbian、Linux、Windows Mobile、Mac OS X、Android、Research in Motion（RIM）等。依據 Canalys 市調機構的最新統計資料，2009 年第二季全球開放式系統的市占率，Symbian 為 50.3%，黑莓機的 RIM 為 20.9%，iPhone 的 Mac OS X 為 13.7%，Google 的 Android 為 2.8%，微軟的 Windows Mobile 為 9%，可見 Symbian 系列之手機占有率超過一半以上，如圖 1 所示，為全球最主要系統之一，此外，根據 Gartnet 市調機構統計，2009 年第二季全球手機銷售總計 2.861 億支，智慧型手機銷售量突破 4096.28 萬支，可見智慧型手機除了功能眾多之外，同時也深受消費者的喜愛[2][5]。

2009 年 8 月大陸中國經濟網站也指出，智慧型手機的作業系統平台，提供第三方業者競相開發相關應用軟體，滿足廣大用戶各方面需求，但是這種開放式架構，卻可能被駭客拿來使用，開發惡意程式、病毒，竊取或破壞手機內儲存之資料，例如手機不斷收發簡訊、不斷的當機、耗電量增加、無法收發話等情況，這些都有可能是手機中毒等現象[1]。近來國內新聞媒體的報導屢次出現「手機竊聽軟體」一詞，該等軟體最主要的功能，即監聽語音談話內容、監看文字圖片簡訊，此等軟體可視為惡意程式的一種。因此，有心人士將惡意程式改寫或包裝後，誘使大眾安裝使用，續而進行其他犯罪之可能性無法排除。

3. 手機竊聽軟體功能簡介與實驗

行動電話作業系統公司 Symbian Limited 對智慧型手機，開發出 Symbian 系列作業系統，主要採用的廠商為 NOKIA 和 Sony Ericsson，其中 NOKIA 採用 Symbian Series60（簡稱 S60）或 Symbian Series 40（簡稱 S40），Sony Ericsson 採用 UIQ，這兩者之間除了介面不同之外，程式也無法相容。目前主要採用 S60 及 S40 的廠商為 NOKIA，而 Samsung、LG 等廠商也都有支援該系統的手機。智慧型手機的功能強大，手機用戶可以自行安裝對應程式，加上智慧型手機的業者提供程式碼讓用戶自由開發應用程式，所以從網路上都可以搜尋到許多免費的應用軟體和遊戲，均可安裝到智慧型手機上，例如：Fring 語音聊天軟體、N-Game、電子地圖…等。所以，目前網路上已能瀏覽到有心人士開發出具有竊聽或盜取簡訊等功能之惡意軟體，如圖 2 至圖 3 所示，顯示出目前竊聽軟體支援的機型，均是針對 S60 和 Windows Mobile 系列的作業系統手機。

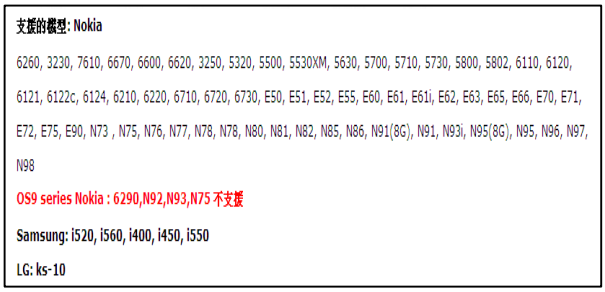

圖 2 手機竊聽軟體支援的機型（Series60）[4]

圖 3 手機竊聽軟體支援的機型（Windows Mobile）[4]

表 1 手機竊聽軟體功能（Series60）[4]

	專業旗艦版	專業版	旗艦版	基礎功能版
現場環境監聽	✓	✓	✓	✓
短信備份	✓	✓	✓	✓
來電去電通知	✓	✓	✓	✓
通話內容監聽	✓	✓	✓	✓
重新啟動或換卡通知	✓	✓	✓	✓
基站位置查詢	✓	✓	✓	✓
重開機	✓	✓	✓	✓
狀況報告	✓	✓	✓	✓
現場環境錄音	✓		✓	
通話內容錄音	✓		✓	
GPS 定位	✓	✓		
關機監聽	✓	✓		

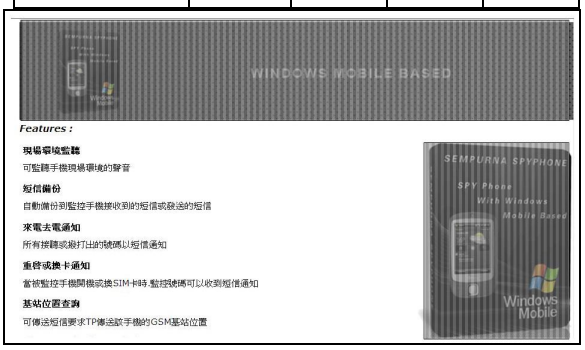

圖 4 手機竊聽軟體功能（Windows Mobile）[4]

從網路上發現，有許多不肖業者在販售「手機監聽」軟體，依功能的不同，其價位均在上萬元左右。經探詢後得知，S60 竊聽軟體共分成四種版本，如表 1 所示。Windows Mobile 竊聽軟體功能，如圖 4 所示，各種功能的說明如下[4]：

1.現場環境監聽（側音）

可以竊聽到現場環境聲音，但被竊聽者不會發現，當有電話發話到被竊聽手機時，或是被竊聽者要撥打電話時，則竊聽過程將主動中斷，以避免被發現。

2.短信備份（簡訊備份）

當被竊聽手機收到簡訊或發出簡訊時，竊聽軟體會將「通話對象」及「簡訊內容」，以文字簡訊(text messages)的方式，寄送到竊聽手機，並自動刪除被竊聽手機中之寄件備份檔，讓被竊聽者無法發現。

3.來電去電通知（主動回報）

當被竊聽手機於發話或受話時，竊聽軟體均會將「通話對象」，以文字簡訊的方式，通知竊聽手機，並自動刪除被竊聽手機中之寄件備份檔，以避免被發現。

表 2 各家電信業者-多方通話服務一覽表（作者整理）

電信業者	2G 系統	3G 系統	設定方法
中華電信	（預設開啟）最多提供六方通話。	（預設開啟）最多提供六方通話。	A、B 通話中，接聽第三方來話，按 2+通話鍵，接通後，在按 3+通話鍵，開始三方通話。
臺灣大哥大	（預設未開啟）初次辦理門號，必須兩個月以上使用紀錄，或超過 3000 元資費。	（預設未開啟）初次辦理門號，必須兩個月以上使用紀錄，或超過 3000 元資費。	A、B 通話中，按 2+通話鍵，在按第三方號碼+通話鍵，接通後，在按 3+通話鍵，開始三方通話。
遠傳、和信	（預設未開啟）	（預設未開啟）最多提供五方通話。	A、B 通話中，按 2+通話鍵，在按第三方號碼+通話鍵，接通後，在按 3+通話鍵，開始三方通話。
亞太電信	（預設未開啟）	（預設未開啟）	A、B 撥通中，按第三方號碼＋通話鍵，接通後，開始三方通話。
威寶電信	（無）	（預設開啟）最多提供五方通話。	A、B 撥通中，按第三方號碼＋通話鍵，接通後，在按 3+通話鍵，開始三方通話。

4.通話內容監聽（語音竊聽）

被竊聽手機開啟「多方通話」服務時（各家電信業者的多方通話服務，如表 2 所示），當被竊聽手機於發話或受話，雙方通話之情況時，則竊聽軟體會將「通話對象」，以文字簡訊的方式，通知竊聽手機，竊聽手機即可選擇是否要發話到被竊聽手機，以三方通話模式，竊聽雙方的談話內容，且當下不會被察覺。

5.重新啟動或換卡通知（自動回報）

當被竊聽手機重新開機或更換 SIM 卡時，竊聽軟體會以文字簡訊的方式，通知竊聽手機，並自動刪除被竊聽手機中之寄件備份檔，避免被發現。

6.基站位置查詢（回報被竊聽者所在基地台位置）

當竊聽手機發送指令簡訊至被竊聽手機，竊聽軟體在收到指令簡訊後，會刪除該則文字簡訊，再將被竊聽手機所在的基地台位置（LAC、Cell ID），以文字簡訊的方式，通知竊聽手機，並自動刪除被竊聽手機中之寄件備份檔，避免被發現。

7.重開機（遠端控制重新開機）

當竊聽者發現被竊聽手機運作有異常現象，需要重新開機啟動手機時，可發送指令簡訊至被竊聽手機，竊聽軟體在接收到指令簡訊後，會刪除該則簡訊，並將被竊聽手機重新開機。

8.狀況報告（手機竊聽軟體狀況報告）

當竊聽手機發送指令簡訊至被竊聽手機，竊聽軟體在收到指令簡訊後，會刪除被竊聽手機中所收到的指令簡訊，同時將目前的狀態（例如現場環境監聽功能是否開啟），以文字簡訊的方式，通知竊聽手機，再自動刪除被竊聽手機中之寄件備份檔，避免被發現。

9.現場環境錄音（現場環境監聽進階功能）

竊聽手機發送指令簡訊至被竊聽手機，竊聽軟體在收到指令簡訊後，會先刪除被竊聽手機中指令簡訊，接著會開啟現場環境監聽的功能，將現場的聲音錄製成音檔，再透過行動網路（GPRS/HSDPA），將該聲音檔案傳送到指定的 Gmail 信箱（竊聽軟體無法傳送到其他業者信箱，主要以 Gmail 為預設對象）。

10.通話內容錄音（通話內容監聽進階功能）

當被竊聽手機於發話或受話時，竊聽軟體均會將「通話內容」錄製成音檔，再透過行動網路（GPRS/HSDPA），將聲音檔案傳送到指定的 Gmail 信箱（竊聽軟體無法傳送到其他業者信箱，主要以 Gmail 為預設對象）。

11.GPS 定位

當竊聽手機發送指令簡訊至被竊聽手機，竊聽軟體在收到指令簡訊後，會先刪除被竊聽手機中收到的指令簡訊，接著開啟 GPS 設備（被竊聽手機必須具有 GPS 功能方能啟動運用），將目前所在的位置資訊，以文字簡訊的方式，通知竊聽手機，並自動刪除被竊聽手機中之寄件備份檔，避免被發現。

12.關機監聽

當竊聽軟體的關機監聽功能啟動後，被竊聽手機在按下關機鍵後，便處於休眠狀態，竊聽手機即可透過被竊聽手機的通話設備對現場環境進行竊聽，聽取現場環境聲音。

經由上述介紹的竊聽軟體功能，得知只要發送指令簡訊到被竊聽手機，就可輕易對該手機進行全般功能的控制，且被竊聽者當下均無法立即察覺。本局科技犯罪防制中心人員多次與外勤隊人員配合偵辦案件，查獲相關手機竊聽軟體，為能剖析坊間手機竊聽軟體實際運作方式，在採取必要之安全措施下，透過實驗模擬、軟體安裝與通聯資料分析等方法，針對微軟 Windows Mobile 手機系統進行測試，實驗結果如下：

竊聽軟體被安裝在被竊聽手機 0916-21****上，並指定 0987-00****為竊聽者。當不知情之第三人 0933-27****發送簡訊到被竊聽手機 0916-21*****時，則竊聽手機 0987-00****也同時收到一模一樣的簡訊內容和發話者（第三人）手機號碼（0933-27****），如圖 5 所示。

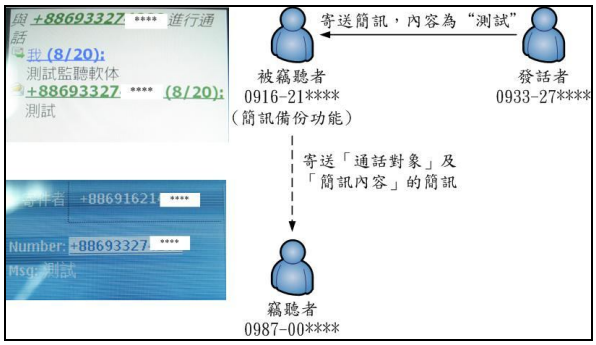

圖 5 竊聽過程示意圖（作者整理）

4. 手機竊聽軟體安裝流程

Symbian S60 和 Windows Mobile 二種系統軟體，屬於性質完全不相容之作業系統，所以竊聽軟體之安裝過程有所差異，接下來，將介紹如何在這兩種作業系統上，安裝竊聽軟體。

4.1 Symbian S60 竊聽軟體安裝流程

Symbian Limited 基於手機系統運作穩定與安全考量，避免用戶安裝到惡意程式，或是應用程式與系統不相容，造成作業系統頻頻當機等問題。當用戶在安裝第三方應用程式時，均需經過該公司官方數位簽章認證，方能順利安裝到手機系統上。由於竊聽軟體未通過 Symbian Limited 簽章認證，所以如要安裝竊聽軟體，必需先行取得被竊聽手機的機身號碼（IMEI），並透過 Symbian 官方的開發者憑證程式（Symbian Developer Certificate），方可製作出竊聽軟體所需要的憑證。竊聽軟體安裝流程，包含 2 大階段：1.產生手機竊聽軟體 2.安裝手機竊聽軟體，各流程簡述如下：

4.1.1 產生手機竊聽軟體階段

1.執行竊聽軟體產生器，填入手機機身號碼、匯入手機憑證和密鑰，即可產生 main.sis 與 update.sis，如圖 6 至圖 7 所示。這二個檔案之副檔名均為 sis，即為客制化竊聽軟體，它能夠偽裝成一般的應用程式（例如：遊戲軟體或其他工具名稱），讓被竊聽者察覺不出來，此軟體安裝到手機系統上，會偽裝成「收聽廣播軟體（Radio）」（據業者宣稱 Ge○○○or v1.4 版以後，均能任意修改軟體名稱，諸如偽裝成遊戲軟體或其他軟體名稱）。

2.竊聽軟體產生器所產生的竊聽程式，屬於第三方應用程式（非 Symbian 公司官方所開發），必需要再透過 Symbian Signed 官方網站，對程式做簽章認證，方能正常順利安裝到作業系統中。

4.1.2 安裝手機竊聽軟體階段

1.將簽章認證後的竊聽軟體儲存到手機記憶卡中，或寄送服務訊息至被竊聽手機，誘騙連上行動網路（GPRS/HSDPA）下載，並將竊聽軟體安裝到手機上。

2.寄送指令簡訊，包括變更密碼、指定監聽手機門號、竊聽等基本功能設定，如圖 8 所示，設定的流程如圖 9 所示。被竊聽手機收到開頭是「0000」簡訊內容，則竊聽軟體會自動刪除該則指令簡訊，手機也不會顯示有收到任何簡訊，所以，被竊聽者完全不會發現有任何異常簡訊送到。

竊聽軟體不論是否有完成指定的功能設定，都會以文字簡訊的方式通知寄件人，即使是錯誤的指令，也會收到竊聽軟體回覆的文字簡訊。竊聽軟體在寄送文字簡訊後，會自動刪除被竊聽手機中之寄件備份檔，讓被竊聽者無法發現遭到被竊聽的跡象。

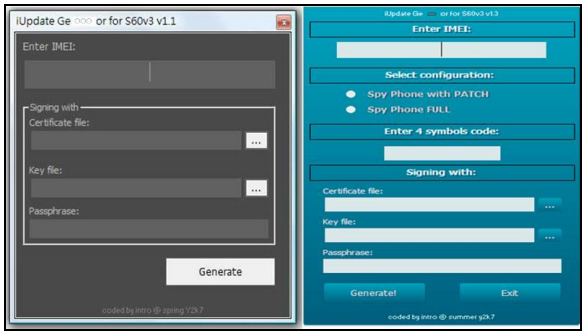

圖 6 手機竊聽軟體產生器（Ge○○○or v1.1 與 Ge○○○or v1.3）

圖 7 手機竊聽程式（main.sis 與 update.sis）

功　能	開啓指令	關閉指令
更改或傳送監控號碼	0000111 +電話號碼	
啓動或關閉所有功能	0000222 1	0000222 0
現場監聽功能	0000333 1	0000333 0
簡訊備份回傳功能	0000444 1	0000444 0
來電或撥出電話通知功能	0000555 1	0000555 0
通話內容監聽功能	0000666 1	0000666 0
開機或更換SIM 卡通知功能	0000777 1	0000777 0
手機定位數字回傳	0000888	無
重新啓動手機	0000999	無
查尋軟體在手機內的設定狀態	0000000	無

圖 8 手機竊聽軟體指令簡訊（適用於 Ge○○○or v1.1）

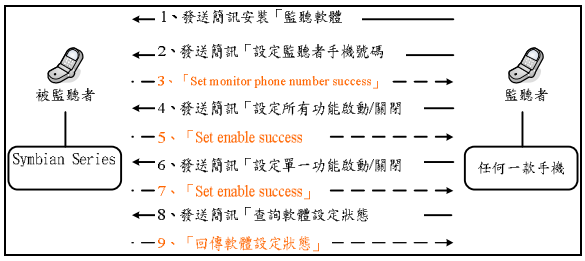

圖 9 手機竊聽軟體設定流程圖（Symbian S60）

4.2 Windows Mobile 竊聽軟體安裝流程

目前，S60 能被安裝竊聽軟體，而微軟旗下 Windows Mobile 作業系統也亦可安裝，甚至發現不需向原廠申請憑證，即可直接安裝到手機中，因此這類手機更容易成為被竊聽對象，竊聽軟體安裝流程如下：

1.竊聽軟體（windowspyphone.CAB）儲存在手機記憶卡中，如圖 10 所示，或寄送服務訊息至被竊聽手機，誘騙連上行動網路（GPRS/HSDPA）下載，並將竊聽軟體安裝到手機上。

2.成功安裝完成後，在設定的「移除程式」內，會看到竊聽軟體被偽裝成微軟的應用程式（Microsoft SetupMapiRule）（解壓縮 windowspyphone.CAB，修改*.xml 程式碼，即可修改偽裝的程式名稱，例如偽裝成 Microsoft Office），如圖 11 所示。

3.客制化的 Windows Mobile 竊聽軟體，需要輸入手機機身號碼到註冊機，取得竊聽軟體的註冊碼，如圖 12 至圖 13 所示。之後，在以簡訊的方式，寄送到被竊聽手機，方能啟動竊聽軟體，如圖 14 所示。

4.其他的指令簡訊，包括變更密碼、指定監聽手機門號、設定簡訊備份功能啟動與否，操作的指令如表 3 所示，設定的流程如圖 15 所示，設定的結果如圖 16 至圖 18 所示。被竊聽手機收到開頭是「0000」簡訊內容，則竊聽軟體會自動刪除該則指令簡訊，手機也不會顯示有收到任何的簡訊，因此，被竊聽者不會發現有任何異常簡訊送到。

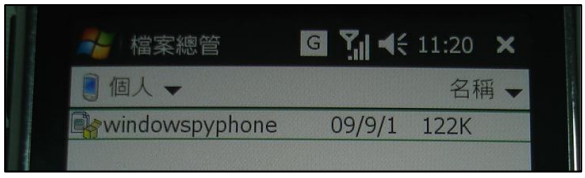

圖 10 儲存在手機中的竊聽軟體

圖 11 手機竊聽軟體被偽裝成微軟的應用程式

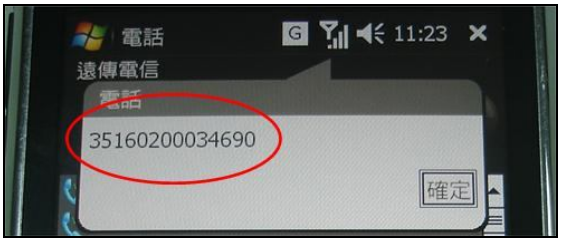

圖 12 被竊聽手機的手機機身號碼

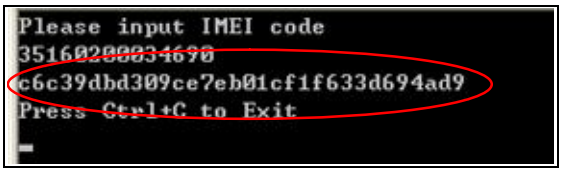

圖 13 Windows Mobile 手機竊聽軟體-註冊碼

圖 14 啟動手機竊聽軟體

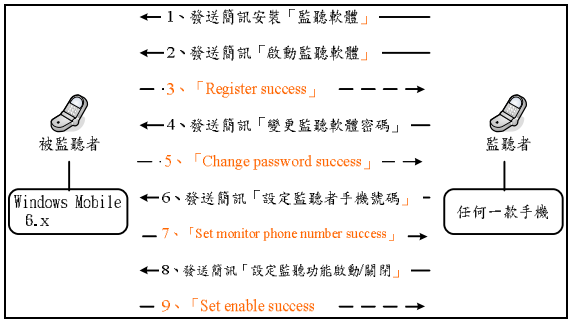

圖 15 手機竊聽軟體設定流程圖（Windows Mobile）

圖 16 變更手機竊聽軟體密碼

圖 17 設定竊聽手機門號

傳送啟動程式訊息　　設定成功訊息

圖 18 設定簡訊備份功能啟動與否

表 3 手機竊聽軟體指令簡訊(適用於 Windows Mobile)

控制碼	註冊指令	註冊碼	預設密碼
0000	0001	****	0000
控制碼	變更密碼	新密碼	舊密碼
0000	0002	****	****
控制碼	監聽手機門號	監聽手機門號	密碼
0000	0003	09xxxxxxxx	****
控制碼	簡訊備份	1 啟動/0 停止	密碼
0000	0004	1	****

4.3 小結

分析上述兩款市面上普遍運用在智慧型手機作業系統上的竊聽軟體，發現大致上功能相仿，並且竊聽軟體不論是否有完成指定的功能設定，都會以文字簡訊的方式通知寄件人，即使是錯誤的指令，也會收到竊聽軟體回覆的文字簡訊。

為避免竊聽行為遭到發現，竊聽軟體在寄送簡訊後，會自動刪除被竊聽手機中之寄件備份檔，讓被竊聽者無法發現被竊聽。

5. 手機竊聽軟體防制與排除作法

5.1 手機竊聽軟體防制作法

透過竊聽軟體實際測試與剖繪歹徒運用竊聽軟體之想法，進一步解析犯罪手法，提出三項防制竊聽軟體解決之道：

1.手機竊聽軟體是客制化產品

智慧型手機系統廠商為保護手機作業系統運作安全與整體效能，對於第三方業者所開發的應用軟體（舉凡本文所提竊聽軟體），均需配合原廠的軟體製作規範，並加入欲安裝標的手機機身號碼，才允許軟體在手機作業系統中運作。由此可知，竊聽軟體如無法取得被竊聽手機機身號碼，則無法完成軟體製作與安裝，也就是說竊聽軟體是客制化的產品，無法單一軟體適用所有對象，而運作主要

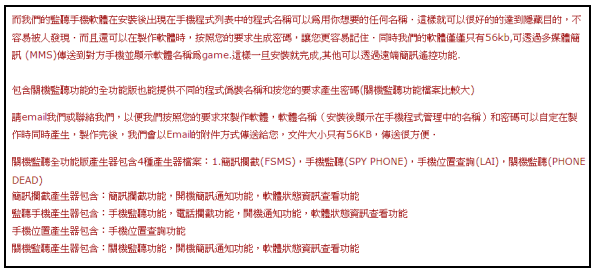

圖 19 手機竊聽軟體的產品說明[4]

關鍵在於手機機身號碼，所以防杜竊聽軟體最好作法，就是不向他人透露自己的手機機身號碼，避免遭到有心人士竊聽。

2.防止手機流落他人之手或接受來路不明手機

為了避免手機遭到非法安裝竊聽軟體，最重要的是手機不離身、不收受來路不明手機，如認為手機可能遭到安裝竊聽軟體，應先將手機送到原廠客服中心，重灌作業系統或自行將手機格式化，還原成出廠原始設定值。

3.避免連接網路下載不明程式誤植入手機竊聽軟體

據販賣竊聽軟體的業者，在網站上展示新一代技術的竊聽軟體，可以任意修改軟體名稱，並且可將程式隱藏在多媒體簡訊（MMS）中，誘騙被害人開啟及安裝，所以對於來路不明之多媒體簡訊或網址連結，不要輕易開啟及下載，以避免被安裝竊聽軟體，如圖 19 所示。

5.2 簡易排除手機竊聽軟體方法

上述的介紹中，可以得知竊聽軟體能偽裝成任何程式，不容易去察覺出自己的手機是否已被安裝。目前，竊聽軟體只能安裝到 S60 和 Windows Mobile 手機作業系統，以下針對這兩種作業系統，被植入竊聽軟體時，簡易的辨識排除方法。

5.2.1 Symbian S60 處理方法

當手機被安裝竊聽軟體後，在手機的程式管理內會看到「Radio」程式名稱（Ge○○○ or v1.1 手機竊聽軟體預設檔名），不過從 Ge○○○or v1.4 之後的版本，可以自行修改程式名稱，所以看到未知的程式名稱，應詳加留意觀察。如果，發覺或懷疑自己的手機，有可能被安裝竊聽軟體，建議使用下列的方法：

1.輸入手機指令還原出廠設定

輸入指令『*#7370#』，輸入預設密碼為『12345』，將手機恢復成出廠設定。此功能會將手機格式化，刪除掉通訊錄、簡訊…等相關

個人資料，所以，在輸入指令前，要先將個人資料備份到記憶卡。

2.送到 NOKIA 客戶服務中心

將手機送到 NOKIA 客戶服務中心或是 NOKIA 授權服務中心，重灌手機作業系統。

3.編寫指令簡訊測試手機

利用其他的手機，編寫簡訊內容為「0000000」發送到自己的手機，如果有被竊聽的話，就收不到該則簡訊，被竊聽者也不會查覺到有簡訊寄送到手機。因為，竊聽軟體收到「0000XXX」簡訊時，會將該則簡訊刪除，不論是否有完成指定的功能設定，都會以簡訊的方式通知寄件人，並啟動指定的功能，例如查詢竊聽軟體的狀態(此方法僅適用於 Ge○○○or v1.1。Ge○○○or v1.3 之後的版本，可以修改指令為 love1111、bady1111)。

5.2.2 Windows Mobile 處理方法

手機被安裝竊聽軟體後，在手機功能選單「系統」中的「移除程式」，會看到檔名為 Microsoft SetupMapiRule（Windows Mobile 手機竊聽軟體預設檔名），如圖 20 所示，不過最新版本的竊聽軟體可以自行修改程式名稱，所以看到未知的程式名稱時，應詳加留意觀察。如果，發覺或懷疑自己的手機，有可能被安裝竊聽軟體，建議使用下列的方法：

1.使用「移除程式」功能

開啟「移除程式」，將「手機竊聽軟體」移除。

2.送到原廠客戶服務中心

將手機送到原廠授權服務中心，重灌 Windows Mobile 手機作業系統。

3.編寫指令簡訊測試手機

利用其他的手機，編寫簡訊內容為「0000 0002 1111 0000」發送到自己的手機，如果有被竊聽的話，就收不到該則簡訊，被竊聽者不會查覺到有簡訊寄送到手機。因為，竊聽軟體收到「0000」簡訊時，會將該則簡訊刪除，不論是否有完成指定的功能設定，都會以簡訊的方式通知寄件人，並啟動指定的功能，例如修改監聽軟體的密碼。

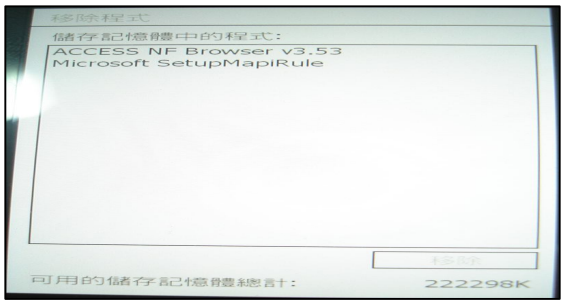

圖 20 Windows Mobile 手機竊聽軟體

5.3 非必要關閉三方通話服務

不論是 S60 或 Windows Mobile 手機作業系統，如果竊聽軟體要竊取語音談話內容，就必需將被竊聽門號開啟「三方通話」服務，才能聽到語音談話內容。所以沒有三方通話服務需求的用戶，應主動與電信業者聯絡，將該服務關閉，才不會被有心人士所竊聽。

5.4 留意觀察電信帳單是否有異常現象

對於疑似被植入竊聽軟體的手機，可以從電信帳單中觀察是否有異常的現象，例如簡訊費用異常增加（竊聽軟體在設定和竊聽的過程中，會大量的寄送文字簡訊給竊聽手機，造成被竊聽手機的簡訊費用增加）、行動網路費用異常增加（使用來傳送錄音檔案，會造成網路連線費用提高），即可研判該手機有可能被植入竊聽軟體。

5.5 遭非法竊聽可從通聯紀錄中查知

對於疑似被植入竊聽軟體的手機，可以從通聯紀錄中查知是否有異常的現象，例如大量寄送簡訊到單一行動門號（竊聽軟體寄送簡訊給竊聽手機，告知設定是否成功和被竊聽手機的現況），或是雙向通聯中出現三方通話的現象，即可研判該手機有被植入竊聽軟體。

為解析遭非法植入竊聽軟體之通聯紀錄，經調閱通聯紀錄可以發現竊聽者之門號，圖 21 為 0933-27****模擬遭竊聽之雙向通聯紀錄，一開始，用戶 B（0987-00****）發話給用戶 A（0933-27****）。由於，用戶 A 有開啟三方通話服務，即使用戶 A、B 通話進行中，用戶 C（0917-51****）也可以發話給用戶 A，同時進行三方通話。從通話時間可以發現到，用戶 A、B 的通話時間為 17:14:21 至 17:14:54，共 33 秒；用戶 C 在 17:14:37 發話進入，是在用戶 A、B 通話期間，據以研判這三個用戶在進行三方通話，故通聯紀錄中可以找出真正竊聽者的行動電話號碼。

始話時間	真實結束時間	通話秒數	對象	調閱號碼	IMEI	通話類別	對象	通話對象	解釋
2009-09-24T17:14:21.000	2009-09-24T17:14:54.001	33	A	93327 ····	35935002262 ····	受話	B	98700 ····	B打給A
2009-09-24T17:14:22.000		33	A	93327 ····		受話	B	98700 ····	通聯多出來
2009-09-24T17:14:37.000	2009-09-24T17:14:55.001	18	A	93327 ····	35935002262 ····	受話	C	91751 ····	C打進來A開啟三方通話
2009-09-24T17:14:38.000		17	A	93327 ····		受話	C	91751 ····	通聯多出來

圖 21 雙向通聯紀錄

6. 結論

現代智慧型手機，如同小型電腦可以隨身攜帶，也可以任意從網路下載軟體來使用，諸如：股市看盤軟體、遊戲軟體、RSS 新聞群組軟體、通訊軟體等，而竊聽軟體的濫用將不再侷限於徵信業者使用，不法人士如濫用透過服務簡訊，誘使民眾開啟上網下載安裝後，手機可能面臨所有的通話內容、簡訊曝光之可能，其要掌握被害人行蹤及動向，則易如反掌，如圖 22 所示，網路上充斥各種智慧手機軟體，但不知情民眾下載這些來路不明可能偽裝為應用程式的惡意軟體，成為將來資通問題與個人資料外洩之隱憂。

經由上述的竊聽軟體功能探討與實驗後發現，目前手機機身號碼是竊聽軟體能否順利安裝執行的關鍵。故不論竊聽軟體技術如何提升，只要遵循本文所提之「手機竊聽軟體防制作法」，即可避免被有心人士趁隙安裝及竊聽。並且「留意觀察電信帳單是否有異常現象」，來研判手機是否有被植入竊聽軟體的可能。如果，發覺或懷疑自己的手機，有可能被植入竊聽軟體時，可使用本文所提之「簡易排除手機竊聽軟體方法」解除疑慮及移除竊聽軟體，阻絕被監控的風險。

圖 22 手機網站上充斥形形色色手機軟體

參考文獻

[1] 中國經濟網，***手機中毒被遙控 自動訂制數十種服務***，2009 年 8 月 10 日，http://big5.ce.cn/cysc/communications/yjdt/200908/10/t20090810_19557668.shtml。

[2] 今日新聞，***破景氣魔咒 慧型手機銷量逆勢成長***，2009 年 8 月 13 日，http://www.nownews.com/2009/08/13/91-2491206.htm。

[3] 自由時報，***抓姦聘假二奶 徵信社 A 大老婆***，2009 年 8 月 14 日，http://tw.news.yahoo.com/article/url/d/a/090814/78/1p0t8.html。

[4] 手機監聽軟體，http://x-○○hone.com/cn/。

[5] DJ 財經知識庫，***Canalys：宏達電北美智慧型手機市佔降至 5.6%***，2009 年 8 月 19 日，http://www.funddj.com/KMDJ/News/NewsViewer.aspx?a=6eb9f170-09a6-417d-810e-651821df74e2。

[6] Mobile Telephone History，http://www.privateline .com/PCS/history8.htm.

[7] 霍華德、瑞格德 (Howard Rheingold) 著，張逸安譯，***聰明行動族***，聯經出版公司，台北，2004。

[8] Mark Weiser, ***The Computer for 21th Century, Scientific American***, September 1991.