十種手機防毒軟體的效能評測

溫倩苓 林盈達
國立交通大學資訊科學系
300 新竹市大學路1001號
9-30-2011
E-MAIL：Chienling.cs00g@nctu.edu.tw, ydlin@cis.nctu.edu.tw

摘要

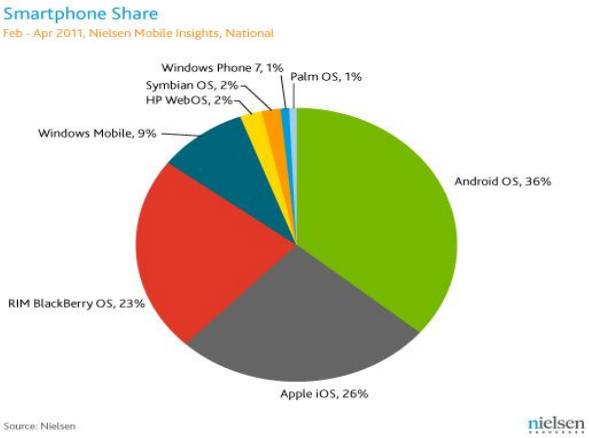
隨著網路與 3G 網路介面的普及，智慧型手機已如雨後春筍般地佔據手機市場並成為民眾生活的重心，因此手機安全與對電池之耗電是目前受注目的議題。手機與電腦安全都是惡意程式藉由檔案交換資料的同時藉機侵入電腦，電腦安全之檔案交換資料的主要來源為外接儲存裝置以及網路下載，相較於此，手機安全交換資料的來源則主要為網路下載。在本文中，我們將針對手機安全與防毒軟體掃描對電池之耗電這兩項議題對目前較多人使用的十種防毒軟體做評比，其評測方法為比較已安裝防毒軟體的掃描耗電、惡意程式偵測率及系統完整掃描時間這三方面的測試結果，選出此次測試最佳的防毒軟體。由測試結果可得知，在掃描耗電方面，DoctorWeb、NetQin、Norton、AegisLab 這四家防毒軟體的耗電比最不耗電的防毒軟體多 80%；在惡意程式偵測率方面，DoctorWeb、Kapsersky 的偵測率最好，皆為 65%；在系統完整掃描時間方面， DoctorWeb、Kapsersky 的掃描時間皆高於最短掃描時間之防毒軟體 99%，由於 Kapsersky 的偵測率好且其不再掃描耗電最多的排名之內，因此此次測試最佳的防毒軟體為 Kapsersky。

關鍵字：耗電量, 偵測率, 防毒軟體, 惡意程式

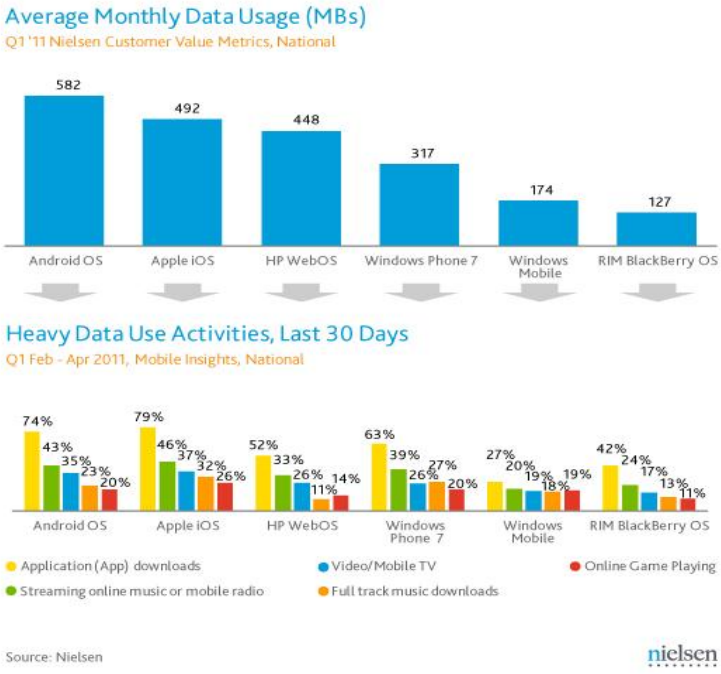
1. 簡介

為什麼手機安全與電池耗電是目前最重視的議題呢？在手機安全方面，手機搭載著網路熱潮，已漸漸成為一台攜帶型的小電腦，電腦安全的漏洞主要在於惡意程式透過外接儲存裝置（例如：隨身碟、光碟、磁片）與他台電腦交換資料時而交互感染，或是透過網路下載的方式感染電腦。相較之下，手機的外接儲存裝置（例如：SD 卡、SIM 卡）較少與他台手機交換資料，因此手機安全的漏洞著重於惡意程式透過網路下載的方式感染手機，然而伴隨著智慧型手機對網路的依賴性逐漸增高，手機安全也成為目前最發燒的議題。另一方面，根據全球知名調查公司尼爾森（Nielsen）在 2011 年 2 月到 4 月的數據顯示[1]：目前手機市場的市占率以 36%的 Android 作業系統位居第一，其次則為 26%的 Apple iOS 系統與

23%的黑莓機的作業系統，如圖一所示。由此可見智慧型手機的兩大作業平台（Android、iOS）已漸漸佔領手機市場。另一方面，Android 作業系統的開放性使得應用軟體數量遽增，更吸引了許多駭客開發 Android 作業系統上的惡意程式，並發佈於 Android Market 中以達到惡意干擾或傳送手機資料至遠端伺服器等危害。再加上調查公司尼爾森（Nielsen）在 2011 年第一季的手機流量使用狀況又以Android平台上的流量為最多，如圖二所示，不難發現危險已漸漸逼近使用者，因此更需要選擇一個好的防毒軟體來監測手機是否受到惡意程式的侵襲。在電池耗電方面，手機電池不如桌上型電腦有交流電持續供應電力，因此一個好的防毒軟體須具備良好的偵測率且不會成為手機之電池耗電的過度負擔。



圖一：2011/02-2011/04 時期
手機平台市占率



圖二：2011 年第一季的手機流量使用狀況

評測方向

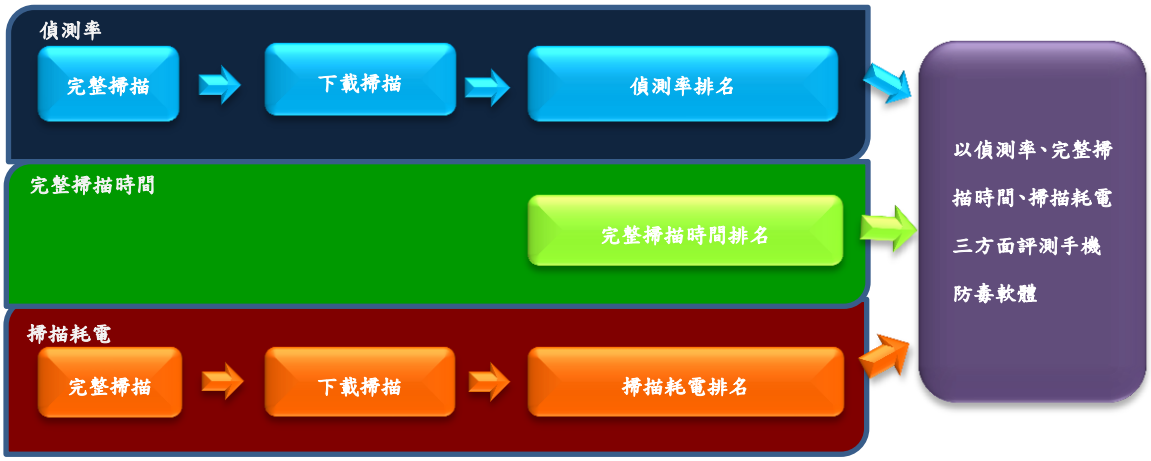
針對這兩項議題，我們挑選 Android market 上較多人下載的前十家免費手機防毒軟體(如表一)當我們評測的產品，十家防毒軟體中只有 NetQin、Lookout、AegisLab 三家針對手機惡意程式做防護；其他家為電腦掃毒公司，紛紛意識到手機安全的重要性，進而推出手機防毒軟體。首先，我們以耗電量、偵測率、完整掃描時間這三方面來評測十家防毒軟體，在耗電量與偵測率方面，我們將選擇各家防毒軟體都有提供的完整掃描與手機最常使用的行為來做評測方向。完整掃描是防毒軟體的基本功能，因此完整掃描的耗電量、偵測率及掃描時間對評測防毒軟體為重要依據之一。另一方面，由於智慧型手機對網路的依賴性增高，手機下載掃描則為手機防毒軟體另一項應具備的功能。那麼哪種下載行為最常在手機上使用呢？根據圖二所示，各平台使用流量以應用程式的下載為最多；且如表二所示，手機與電腦最大的差異除了電流來源、平台的不同之外，其次則為下載途徑。手機應用程式的下載途徑主要仰賴於 Android market 下載、gmail 附件下載、網頁下載(包括一般網頁下載與二維條碼)，因此整體的評測方法如圖三，耗電量與偵測率都分別以完整掃描與手機下載掃描為評測方向，而手機下載掃描又以 Android market 下載、gmail 附件下載、網頁下載來做測試，最後在整合耗電量、偵測率、完整掃描時間來對十家防毒軟體做評測。

編號	防毒軟體名稱	版本
1	NetQin Mobile Anti-Virus	4.8
2	Trend Micro Mobile Security	1.2
3	Norton Mobile Security	2.1.0.270
4	Kapsersky Mobile Security	9.10.75
5	Lookout Mobile Security	6.0.1
6	360Safe Mobile Safe	1.9.6
7	Doctor Web For Android Light	6.00.8
8	AegisLab EigsMobile Anti-virus Security	0.4.24
9	HAURI ViRobot Mobile	1.6.0.1103
10	AVG Anti-Virus Free for Android	2.8.1

表一：手機防毒軟體列表[2]

項目			手機	電腦
電流			直流電	交流電
平台			1. Symbian 2. Research In Motion 3. iPhone OS 4. Android 5. Microsoft Windows Phone 6. Linux	1. Linux 2. Windows series 3. Vista 4. Mac
惡意程式感染途徑	外接儲存裝置		隨身碟	隨身碟/磁片/光碟(CD、DVD)
	網路連接途徑		Internet WiFi/GPRS/EDGE[3]	Internet WiFi
	網路行為	下載	1. 一般網頁 2. Gmail附件 3. Market 4. 二維條碼 Beetagg Datamatrix QR-Code	1. 一般網頁 2. 電子郵件附件
		其他	檔案傳輸	檔案傳輸
	其他		藍芽 SMS/MMS簡訊 SIM 卡	藍芽

表二：手機與電腦的比較表



圖三：整體評測方法流程

2. 評測方法

評測項目

民眾選擇防毒軟體時，除了重視該防毒軟體偵測率的優劣外，另一個重視的是：安裝該防毒軟體後，是否會造成手機耗電增加等相關議題。為釐清耗電量與偵測率的關係，如表三所示，我們將以完整掃描與手機下載掃描為評測方向，並擬定幾項待觀察的測試項目，其中，每個測試項皆分開測試。

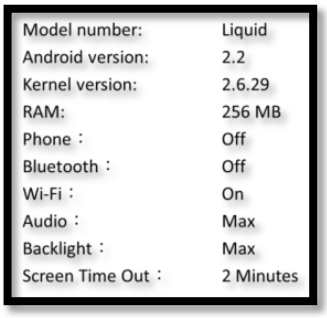
測試領域	測試項目	測試內容
耗電量	完整掃描	完整掃描的瞬時耗電量
	下載掃描	1. Android market 下載 2. gmail 附件下載 3. 網頁下載
偵測率	完整掃描	完整掃描的偵測率
	下載掃描	1. Android market 下載 2. gmail 附件下載 3. 網頁下載

表三：評測項目

評測環境

手機平台

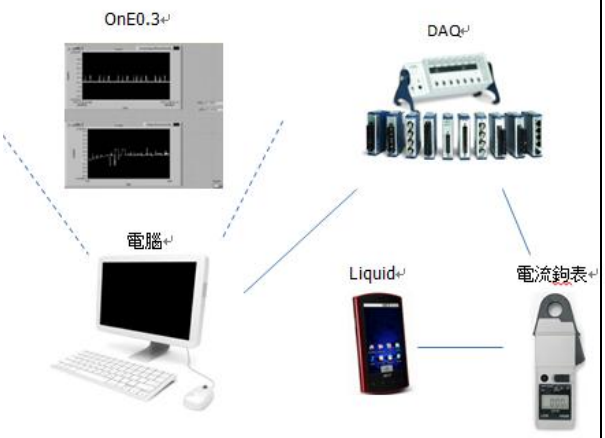
因為手機的背景光、聲音大小都可能會影響電池的使用量，因此在測試前我們須將手機的一些基本條件固定，其固定條件如圖四所示：禁止手機撥接電話、關閉藍芽、聲音最大、背景光最亮、待機時間為兩分鐘。



圖四：手機基本設定

工具

如表四所示，在耗電量測試方面，將 DAQ[6]與電流鉤表連接，再把電流鉤表鉤住手機電池與手機接腳的連線。再來，電腦透過 DAQ 取得電流鉤表所量測的電流值，並使用應用程式 OnE0.3[5]將電流值顯示於圖表且匯出 excel 檔即可取得電流值。在偵測率測試方面，將手機連上無線網路，即可開始進行量測。

測試領域	工具	環境的架設
耗電量	1. 已安裝應用程式 OnE0.3 的電腦 2. DAQ 連結電流鉤表 3. Android 平台的手機	
偵測率	1. Android 平台的手機 2. 無線網路	

表四：測試工具列表

評測方法

◆ **耗電量**

將手機電池與手機金屬接腳的連線延長，用掛勾電表量取電流值並用電腦透過 DAQ 去抓取掛勾電表的電流數據，每次數據都量五次再取平均值。

◆ **偵測率**

完整掃描

惡意程式樣本的來源為網路上公開惡意程式樣本的網站[4]，那些樣本已被認為是 Android 平台上的惡意程式，將其放入 SD 卡中，在只安裝一家防毒軟體的手機上觀察是否有偵測到 SD 卡中的惡意程式。由於此測試手機無法將病毒檔放入系統中做掃描，因此我們只能將其放入 SD 卡中做掃描，也由於此限制，我們只針對有支援 SD 卡掃描的防毒軟體（十家防毒軟體中有六家有支援 SD 卡掃描）來做測試。

下載掃描

惡意程式樣本的來源為網路上公開惡意程式樣本的網站[13]，那些樣本已被認為是 Android 平台上的惡意程式，將其放入 gmail 附件與網頁下載。每一次下載所使用的手機都只安裝一家防毒軟體，透過一一下載附件或網頁上的檔案來觀察防毒軟體是否有偵測到惡意程式。

3. 評測結果

此篇報告欲得知防毒軟體偵測率與掃描耗電之關係，透過量測結果將可得知：哪幾家防毒軟體在完整掃描或下載掃描時最耗電？各家防毒軟體在完整掃描的時間為何？哪幾家防毒軟體對惡意程式的偵測率較好？而在總結，我們將會交叉比對這些問題的結果，選出最此次測試中最佳的防毒軟體。

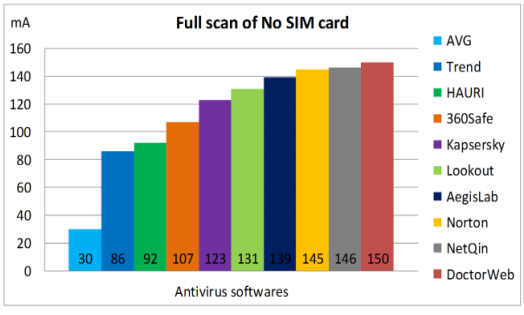
耗電量

完整掃描

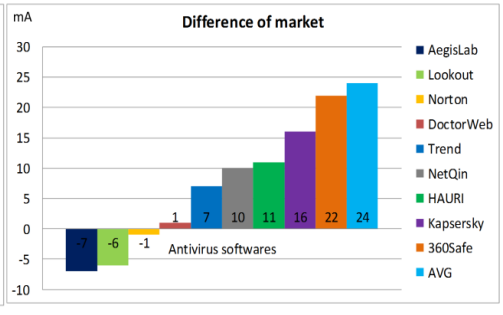
在 30 秒的瞬時耗電量測中，如圖五所示，DoctorWeb、NetQin、Norton、AegisLab 這四家防毒軟體的瞬時耗電值比較大，而 AVG 最小，比最耗電的防毒軟體少 80%。

下載掃描

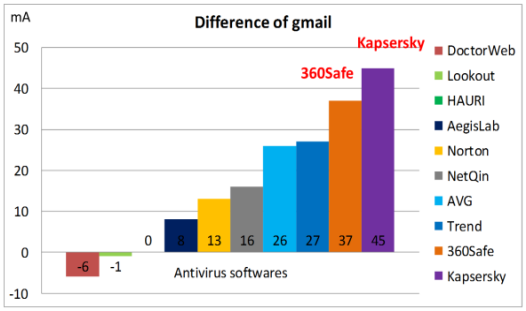
針對下載掃描我們選擇了三項較常使用的下載途徑，分別為 Android market 下載、gmail 附件下載、網頁下載。根據我們的測量結果（圖六到圖八）發現 Android market 下載的耗電差異不明顯，AVG 為偏高；gmail 附件下載與網頁下載都以 Kapsersky、360safe 為最高，皆高於最少耗電之防毒軟體 113%、116%。



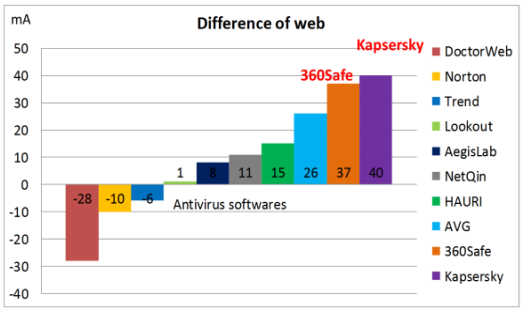
圖五：完整掃描的瞬時耗電量



圖六：Android market 下載的耗電量



圖七：gmail 附件下載的耗電量



圖八：網頁下載的耗電量

完整掃描時間

不同的完整掃描時間，耗電值可能也會有所差異，因此為使量測結果更貼近於真實，針對完整掃描我們也加入時間的考量，圖九為各家防毒軟體掃描的時間，時間最久高達八分鐘，最快則不到三秒。由表五可知道掃描時間又以 DoctorWeb、Kapsersky 為最久，皆高於最短掃描時間之防毒軟體 99%。

1.	NetQin MobileAnti-Virus	about 10 sec (not sure)	
2.	Trend Micro Mobile Security	about 3 sec	
3.	Norton Mobile Security	about 10 sec	
4.	Kapsersky Mobile Security	Full: about 6 minute	Memory: about 9 ~ 60 sec
5.	Lookout Mobile Security	about 30 ~ 45 sec	
6.	360Safe Mobile Safe	about 10 ~ 15 sec	
7.	Doctor Web For Android Light	Full: about 8 minute	Quick: about 3sec
8.	AegisLab EigsMobile Anti-virus Security	about 3 sec	
9.	HAURI ViRobot Mobile	about 3 sec	
10.	AVG Anti-Virus Free for Android	about 20 sec	

圖九：各防毒軟體完整掃描的時間

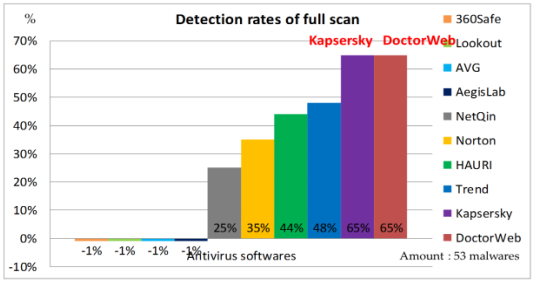
Rank	Full scan
1	Doctor Web
2	Kapsersky
3	Lookout
4	AVG
5	360safe
6	NetQin & Norton
7	AegisLab & Trend & HAURI

表五：掃描時間的排名

偵測率

完整掃描

由於只能將惡意程式放入 SD 卡做掃瞄，因此此項測試只針對有支援 SD 卡掃描的防毒軟體來做測試。如圖十所示，偵測率百分比為負值的表示此防毒軟體無 SD 卡掃描功能，而其他防毒軟體的偵測率百分比值決定於將 35 隻惡意程式放入 SD 卡中，執行完整掃描後所掃到的數量有多少。結果顯示，DoctorWeb、Kapsersky 的偵測率最好，皆為 65%。

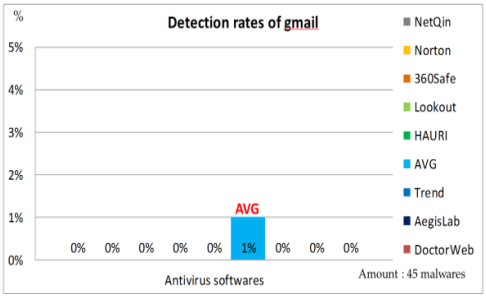


圖十：完整掃描的偵測率

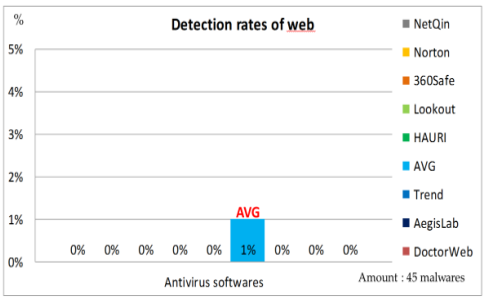
下載掃描

由於 Android market 為開放給民眾下載應用程式的平台，我們無法擅自將惡意程式放入，因此偵測率在下載掃描這部分只針對 gmail 附件下載與網頁下載來做測試。如圖十二與圖十三所示，在 45 隻惡意程式中只有 AVG 掃到 1 隻惡意程式。探究其原因，由於此 45 隻樣本與完整掃描的樣本重複，但同樣的樣本在完整掃描中被偵測得到，因此我們排除惡意程式樣本之選擇有誤，由此可推測目前手機防毒軟體在完整掃描資料庫之病毒碼比下載掃描資料庫之病毒碼還要完善。

註：由於 Kapsersky 的免費版停止使用，所以此次測試不包含 Kapsersky。



圖十二：gmail 附件下載的偵測率



圖十三：網頁下載的偵測率

4. 總結

隨著惡意程式逐漸增加，比起防毒軟體在手機上的耗電問題，民眾更在意防毒軟體是否能確實的掃描到惡意程式，因此我們以惡意程式的偵測率為主要評測因素。根據我們的偵測率量測結果顯示 DoctorWeb 與 Kapsersky 這兩家手機防毒軟體的偵測率比較好。另一方面，我們發現偵測率與完整掃描時間幾乎成正比，因此完整掃描時間這項因素無法提供決定性的依據；後續我們透過 top 工具觀察下載時的程序動向，發現下載掃描的偵測率極低，只有 AVG 這家防毒軟體的偵測率為 1%；其它家為 0%。但是，同樣的一批惡意程式在完整掃描卻能被手機防毒軟體抓取得到，由此我們可推測手機防毒軟體針對下載掃描資料庫內的病毒碼還不齊全或者是尚未加入此功能。除此之外，下載掃描的耗電量主要分布於網頁的抓取、無線網路與 SD 卡資料寫入等程序，因此偵測率與耗電量的下載掃描之測試結果對選擇較佳的防毒軟體來說影響較小。最後，從瞬時耗電量與偵測率的完整掃描之測試結果來看，Kapsersky 這家手機防毒軟體的偵測率高且其不在最耗電的四家防毒軟體之一，如表六所示，因此判斷為本測試最佳的防毒軟體。

5. 參考文獻

[1] nielsenwire: http://blog.nielsen.com/nielsenwire/consumer/android-leads-u-s-in-smartphone-market-share-and-data-usage/

[2] Android 的開放性帶來的衍生問題-10 款 Android 防護軟體的評測結果: http://www.sogi.com.tw/newforum/article_list.aspx?topic_ID=6172147

[3] Jerry Cheng , Starsky H.Y. Wong , Hao Yang , Songwu Lu, SmartSiren: Virus detection and alert for smartphones, Proceedings of the 5th international conference on Mobile systems, applications and services, June 11-13, 2007, San Juan, Puerto Rico.

[4] malware dump: http://contagiodump.blogspot.com/2011/03/take-sample-leave-sample-mobile-malware.html

[5] OnE0.3, LabVIEW Tool

[6] National Instruments: http://www.ni.com/dataacquisition/