Androbug: Android 應用程序之安全漏洞分析系統

林禹成 [1]
miles.linyu@gmail.com
歐捷登 [1]
ngeoucheeden@gmail.com
孫宏民 [2]
hmsun@cs.nthu.edu.tw
[1] 清華大學 資訊系統與應用研究所
[2] 清華大學資訊工程學系

摘要

在台灣，每天有超過 4000 部 Android 手機被攻擊。經統計，更是有超過 80%的 Android 應用程序都有假的版本（他們可能是惡意軟件）[8]。雖然在市場上已經存在了許多殺毒軟件但大多數都只專注於分析惡意軟件和檢測惡意軟件。

而然由於 Android 系統的設計特性，惡意軟件並不一定是直接攻擊而是可以利用其他應用程序自身存在的一些安全漏洞（這是沒有惡意的，但應用程序自身存在的一些安全漏洞使得黑客可以通過這些安全漏洞獲得好處）。就算是知名的應用程序如 Facebook[13]，WhatsApp[14]，Evernote[11]等也有安全漏洞問題存在。

台灣法律更是規定每洩漏一個用戶個資將罰款 500 元至 20,000 元[7]。可見我們並不只需要考慮到惡意軟件還需要考慮到正常應用程序的安全問題。可是大部分的安全專家並不熟悉手機的安全問題（他們一般熟悉在桌面上的安全問題）。

本論文專注於尋找行動設備之應用程序的安全漏洞（安全問題或錯誤）。我們構建了一個高效率的智能系統名為 Androbug，只需要輸入應用程序的 APK 檔案，系統將會輸出應用程序的安全漏洞之報表。

關鍵詞：Android，行動設備，應用程序，漏洞，檢測

壹、前言

由於 Android 系統的設計，每一個應用程序都是相互獨立的。每一個應用程序都運行在一個獨立的虛擬機內，並擁有自己獨立的沙盒和資料庫（SQLite 的）。因此，每一個應用程序都被隔離。這意味著一個應用程序將無法從另一個應用程序獲得任何訊息，文件，資料庫，access token，用戶名，密碼，訪問權限等等。但是，如果一個正常的應用程序患有安全漏洞，應用程序在行動設備有或無惡意應用程序的情況下將可

能承受資訊洩漏或資訊竄改，非法訪問等安全風險。

這些安全漏洞都有可能造成嚴重的後果如應用程序 SSL 誤用[6]使得黑客可以使用 Man-in-the-middle 來攻擊，讓 SSL 的保護失去了意義。Content Provider[5]和對外開放元件(exposed component) [4]等可以讓黑客進行非法訪問造成資訊洩漏和資訊竄改等安全風險。

據統計在 2014 年 7 月 Google Play 上已經有高達 130 萬個應用程序[12]。每用戶的手機都具有多個應用程序，其中更是有一些涉及重要個資的應用程序如銀行應用，通訊軟件等。知名應用和預設應用更是存在在大量的手機上，這些應用程序都是黑客們的主要攻擊目標。若這些應用程序存在著某些安全漏洞讓黑客可以達到目的將造成多少損失？

更值得注意的是在行動設備上的應用程序之更新問題，從應用程序更新到使用者更新應用這一過程所需的時間造成的後果就是就算應用程序已經更新修復問題但使用者和開發商並不會馬上脫離危險，損失將依然持續一段時間。

我們的目標就是提供一個高效率智能系統可以檢測出應用程序所有安全漏洞的系統。讓應用程序在上架前就能夠避免安全漏洞問題，減少使用者和開發商的風險和損失。

貳、相關研究

1.Android 應用程序

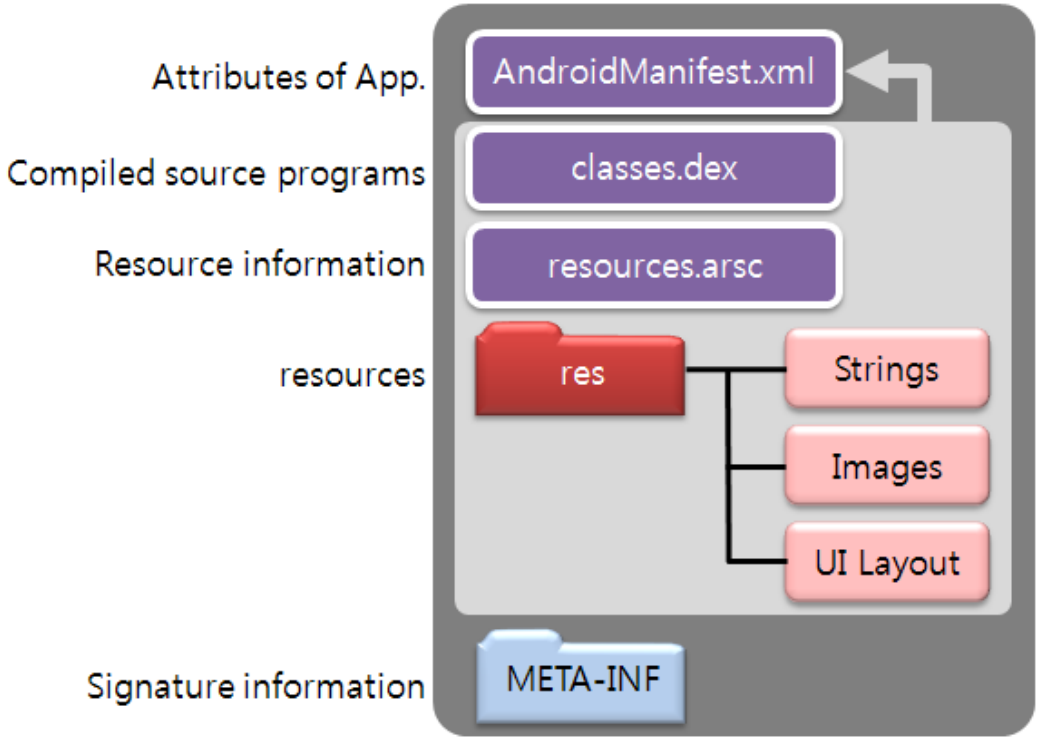
應用程序包含：JAVA 編譯碼(classes.dex) ，資源文件夾 res (字串，圖像和 UI 畫面，Resources.arsc 包含資源相關的信息，META-INF 持有數位簽名的文件。(如**圖一**)

2.反編譯

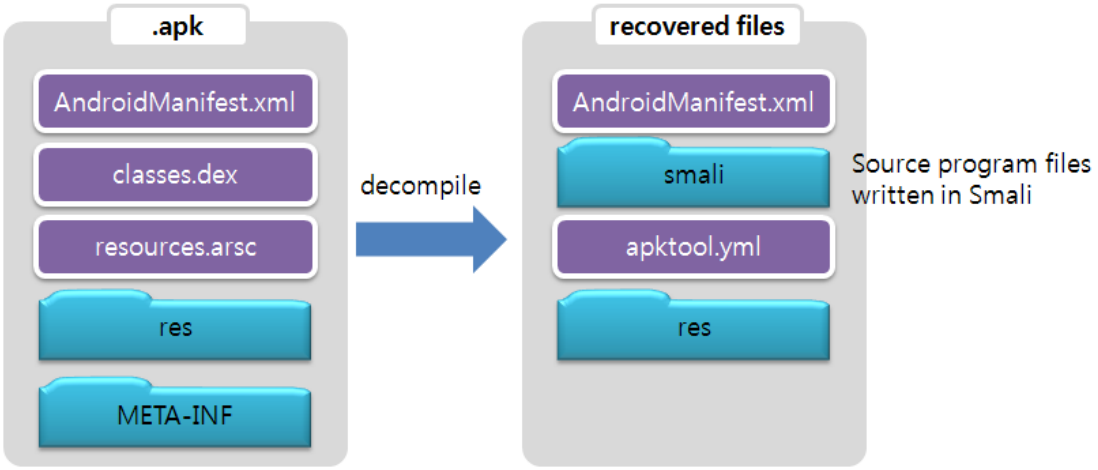
有關 Android 應用程序的反編譯工具有很多如 Dedexer，ApkManager，apktool...等等都可以把應用程序內的 classes.dex 文件反編譯出可看/分析代碼(反編譯細節如**圖二**)。

3.安全漏洞

我們的系統採用了多本資訊安全方面的書籍[1][2][3]和多個 Android 資訊安全方面的研究文章[4][5][6][15]作為檢測標準（詳情請參考第參節）。



圖一：Android 應用程序架構



圖二：Android 應用程序反編譯動操作（使用 apktool 的情況下）

參、安全漏洞

我們只需要輸入應用程序的 APK 檔案(不需原始碼，可有下載的 APP 取得)，系統會自動使用反編譯技術進行反編譯然後靜態分析各種安全漏洞：

1.錯誤設定

以多本 Android 安全教科書的安全知識來做分析。通常是新手常犯的錯誤。

2.版本差異

在不同的 Android 版本有不同的情況，例如 Google Cloud Messaging (Push Message) 只支持 Android SDK 8 以上[9]。因大量行動設備都使用不同的系統版本而各版本及功能都可能存在著一些差異，很容易被工程師所忽略。

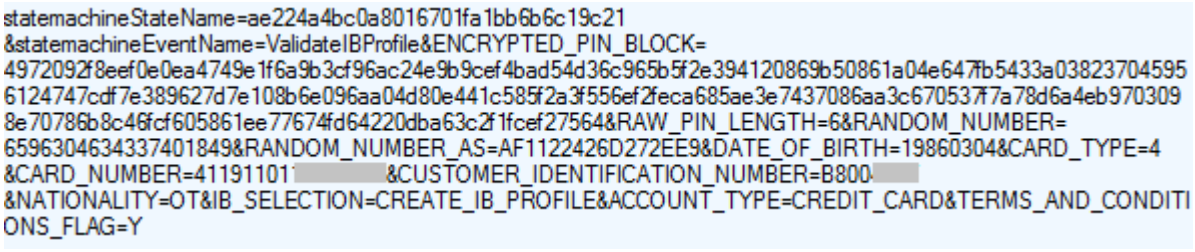
3.SSL 安全漏洞[6]

錯誤使用可能導致 SSL 無效，應用程序將會承受 Man-in-the-middle 之攻擊風險。檢測哪些網絡活動有使用 SSL 保護，哪些沒有。

我們發現了很多銀行都有這方面的問題導致用戶登錄過程完全被第三方監控。如**圖三**

4.Content Provider 安全漏洞[5]

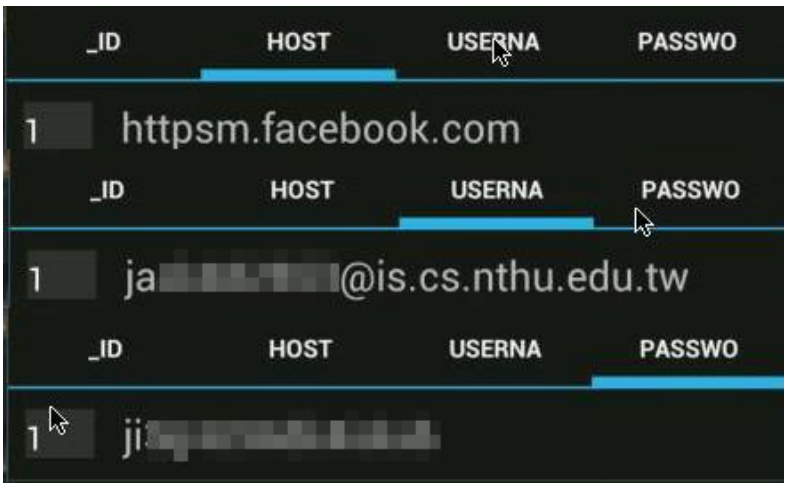
5.



圖三：某銀行洩漏用戶註冊資料

檢測應用程序是否有用到 Content Provider，有沒有對外開放，有沒有使用安全權限被保護起來。

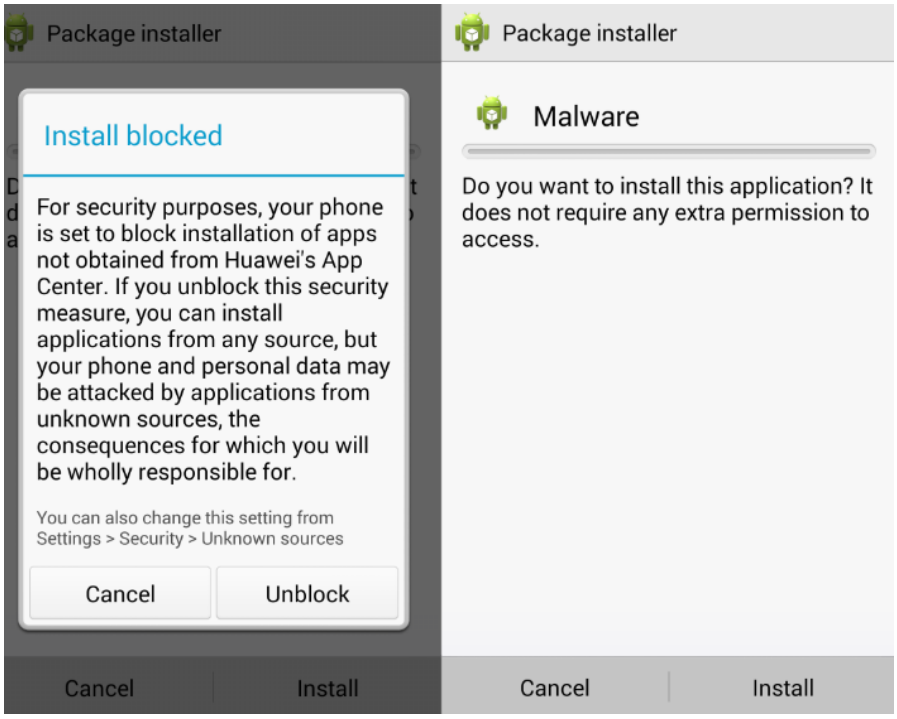
這方面也有很多大公司的案例如 Microsoft 的 Bing 會洩漏它瀏覽器的 Cache，裡面包含了使用者使用 Bing 的瀏覽器來登錄時的賬密和 access token。如**圖四**



圖四：Microsoft Bing APP 資料庫存儲的帳密

6.Exposed Component 安全漏洞[4]

列出所有對外開放的元件。這些元件可能會被黑客利用，如華為的系統應用程序(Package Installer) 因對外開放並接受外來的一個值用於設定導致黑客可以繞過系統的第三方應用程序安裝檢查(黑客可以假裝是幫助用戶從 Google Play 下載正版應用程序但實際上是從第三方下載假的應用程序，如**圖五**)。



圖五：華為手機 P7 中內建的系統 APP，使得只要是華為的 APP，皆可以繞過華為手機的第三方應用程序安裝檢查，這可能是華為為自己留的後門。

7.網絡安全漏洞(RCE) [10]

檢測應用程序是否具有遠程代碼執行的可能性 - 遠程攻擊風險)。

肆、成果

我們找到多個應用程序的安全漏洞並回報給他們：Facebook，Google，Yahoo! ，Microsoft，Alibaba(阿里巴巴) ，Sina Weibo(新浪微博) ，Evernote，LINE，Badoo，Baidu(百度) ，Tencent(騰訊) ，Twitter，AT&T，Yandex，Adobe，eBay，Sony，Tumblr，Mail.Ru，華為(系統應用) ，MediaTek (預設應用) ，多家銀行。

回報到這些公司的漏洞報告皆得到了廠商的漏洞確認並獲得認可，如**表一**

表一：獲得各公司之認可

公司	認可	漏洞數量	時間
Google	Android Security Acknowledgement	5	2014
Facebook	WhiteHat Security Acknowledgement	2	2014
Evernote	Security Hall of Fame	1	2014
Alibaba(阿里巴巴)	Security Acknowledgement	8	2014/04
Microsoft	Security Acknowledgement	2	2014/5，6
AT&T	Security Hall of Fame	1	2014
Twitter	Security Hall of Fame(通過 HackerOne 平台)	1	2014
Sina Weibo	Security Acknowledgement	3	2014/4
Yahoo	通過 HackerOne 平台	1	2014/5
Badoo	Badoo	2	2014/5
Yandex	Bug Bounty Hall of Fame	2	2014/6，7
Baidu(百度)	通過 Wooyun 平台	1	2014/3
Sony	Hall of Thanks	1	2014
eBay	eBay Classifields branded ‘WhiteHat’	1	2014/5
Adobe	Adobe Product Security Incident Response Team	1	2014/5

伍、結論

行動設備之應用程序的迅速發展讓工程師不僅要競爭應用程序之功能還考驗應用程序之安全/風險。而然我們的研究發現就算已經有不少相關的應用程序之安全研究但依然存在大量有安全漏洞的應用程序，這其中還有知名的應用程序或公司，從資訊洩漏到遠程代碼執行，從通訊軟件到銀行應用，影響範圍和造成的損失都不可忽視。
而造成這些問題除了工程師知識限制還因為應用程序的迅速發展引至難以維護，跟進。所以我們開發一個協助工程師檢測應用程序之安全漏洞的系統將有重大的意義，提升行動設備之應用程序的安全性。

參考文獻

[1] Sheran A. Gunasekera, Android Apps Security, 2012.
[2] Rai, Pragati Ogal, Aoki and Edwin, Android Application Security Essentials, 2013.
[3] Jeff Six, Application Security for the Android Platform, 2011.
[4] Daoyuan Wu, "On the Feasibility of Automatically Generating Android Component Hijacking Exploits," Hitcon X, 2014.
[5] Taenam Cho, Jae-Hyeong Kim, Hyeok-Ju Cho, Seung-Hyun Seo and Seungjoo Kim, "Vulnerabilities of Android Data Sharing and Malicious Application to Leaking Private Information," Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference.
[6] Sascha Fahl, Marian Harbach, Thomas Muders, Matthew Smith, Lars Baumgärtner and Bernd Freisleben, "Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security," OWASP AppSec EU, 2013.
[7] http://www.appledaily.com.tw/appledaily/article/finance/20130429/34983588 (2013/4/29).
[8] http://expressofnews.blogspot.tw/2014/08/24-app.html (2014/8/17).
[9] http://developer.android.com/google/gcm/gcm.html.
[10] https://labs.mwrinfosecurity.com/blog/2013/09/24/webview-addjavascriptinterface-remote-code-execution/.
[11] http://www.securityfocus.com/archive/1/530287 (2013/12/12).
[12] http://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores.
[13] http://thehackernews.com/2013/10/vulnerability-in-facebook-app-allows.html (2013/10/29).
[14] http://techcrunch.com/2014/03/12/hole-in-whatsapp-for-android-lets-hackers-steal-your-conversations/ (2014/3/12).

[15] 胡文君(MindMac) and 肖梓航(Claud Xiao), "Guess Where I am: Android模拟器躲避的检测与应对," Hitcon X, 2014.

[作者簡介]

- 孫宏民(Hung-Min Sun)教授

信箱：hmsun@cs.nthu.edu.tw

電話：03-5742968

領域：資訊安全、密碼學、網路安全、資料壓縮

學歷：國立交通大學博士

- 林禹成

清華大學 資訊系統與應用研究所

碩 101

- 歐捷登

清華大學 資訊系統與應用研究所

碩 102