Security Content Automation Protocol 於iPhone上之應用

陳長明[1] 楊中皇[2]
國立高雄師範大學資訊教育研究所[1,2]
samlflb@gmail.com[1]
chyang@nknucc.nknu.edu.tw[2]

摘 要

隨著資訊科技不斷的向前發展,網路全面化的普及,資訊網路化的時代已經來臨,電腦已經成為人們生活中不可或缺的一部份.但相對的各種網路攻擊也開始活躍,從許多的攻擊案例來看,大部份的攻擊行為都是利用電腦系統軟體的弱點,以及人們忽略掉系統更新的重要性所引起的.不僅使自身重要資料被盜取,對企業而言更是蒙受重大商譽和利益的損失.透過 SCAP 安全自動化協定(Security Content Automation Protocol)的檢核,可讓企業統一控管內部電腦資訊安全性,達到企業資訊安全政策一致化。

由於智慧型手機日漸普及 ,軟體功能也愈趨完善,就像人們手中的小型電腦一樣,根據國際數據公司 IDC 統計智慧型手機作業系統,Apple iOS 市占率僅次於 Android,相對資訊安全也會應運而生,因此本研究提出將 SCAP 的應用在手機作業系統上,以加強並確保其安全性的管控。

關鍵詞：資訊網路化、網路攻擊、SCAP、智慧型手機、資訊安全

1. 前言

早期 Internet 尚未成熟普及發展應用，使用者個人電腦端面對電腦病毒攻擊的防範只要不使用及不安裝來路不明的軟體；並且安裝防毒軟體加上定期更新病毒碼就可以大大減少病毒對於個人電腦的威脅。但隨著網路基礎建設佈建率提高，使用者也慢慢透過 Internet 獲取資訊及彼此相互交流，這對於資訊科技的發展是有很長足進步與幫助，但伴隨而來的資訊安全威脅已經不單單是病毒的攻擊而已，駭客入侵、釣魚郵件/網站、P2P 軟體、即時通訊軟體，導致資料外洩的資安問題層出不窮。近幾年來智慧型手機功能的進步而開始盛行，使用者也漸漸使用智慧型手機來處理日常生活中的事情。

根據國際數據公司 IDC 對於智慧型手機在 2012 年第四季的出貨量和市場份額所做的統計資料顯示，智慧型手機所搭載的作業系統還是以 Android 和 iOS 佔居 1,2 名(圖 1 和圖 2)[2]。根據賽門鐵克第 17 期全球網路安全威脅研究報告指出，2011 年惡意攻擊數量超過八成，而在報告中所強調的 2011 網路安全威脅四大現象其中一項為「行動威脅危及企業與消費者」,內容指出(隨著行動漏洞數量增加，惡意程式作者不僅以行動裝置為目標而重新調整現有惡意程式，更針對獨特的行動漏洞創造特定的惡意程式)。因此若能在漏洞發佈時及相關惡意程式攻擊前，將行動裝置系統漏洞修補起來，這對於行動裝置系統的安全性可將是大大的提高。

Top Five Smartphone Operating Systems, Shipments, and Market Share, 4Q12 (Units in Millions)

Operating System	4Q12 Unit Shipments	4Q12 Market Share	4Q11 Unit Shipments	4Q11 Market Share	Year over Year Change
Android	159.8	70.1%	85.0	52.9%	88.0%
iOS	47.8	21.0%	37.0	23.0%	29.2%
BlackBerry	7.4	3.2%	13.0	8.1%	-43.1%
Windows Phone/ Windows Mobile	6.0	2.6%	2.4	1.5%	150.0%
Linux	3.8	1.7%	3.9	2.4%	-2.6%
Others	3.0	1.3%	19.5	12.1%	-84.6%
Total	227.8	100.0%	160.8	100.0%	41.7%

圖 1 智慧型手機作業系統市場佔有率預測

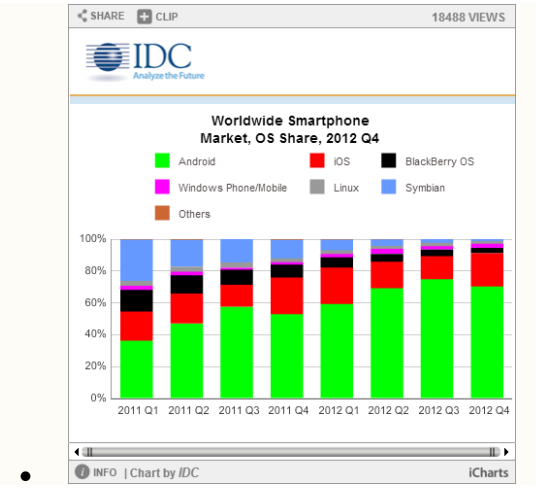

圖 2 智慧型手機作業系統 2012 Q4 市佔率統計

2. 文獻探討

本研究著重 SCAP 安全自動化協定(Security Content Automation Protocol)在 IPhone 智慧型手機上的應用，並以 iOS 作業系統做為研究標的，依據研究所需之相關名詞與定義進行文獻探討。

* 本研究接受國科會編號：NSC 101-2221-E-017-013 研究計畫經費補助

2.1 智慧型手機

隨著科技日新月異不斷的發展，智慧型手機的功能愈來愈強大，許多個人電腦上能處理的事情，智慧型手機也都能做到**[10]**，由於不同的技術和硬體規格，手機可分為三類:(一)基本型(二)進階型(三)智慧型**[4]**，基本型手機具有語音通話和簡訊功能;進階型手機除具有基本型功能外，還增加多媒體功能服務;智慧型手機則是結合進階型手機功能以及個人數位助理(Personal Digital Assistant, PDA)。國際數據資訊公司(International DataCorporation, IDC)對於智慧型手機的定義為，整合行動電話與個人數位助理的行動裝置，除包含基本的語音通話功能外，瀏覽網際網路、收發電子郵件、個人資訊管理(Personal Information Management, PIM)、下載檔案及文件處理等功能。國內資策會產業情報研究所(Market Intelligence & Consulting Institute, MIC)對於智慧型手機也有定義如表 1。

表 1 智慧型手機定義
（資料來源:MIC 研究報告，2002/12/01）

項目	定義
基本功能	具備語音及數據之無線通訊功能，為內嵌式而非外加之模組
語音通訊	具備內嵌式語音通訊功能
數據通訊	具備個人資訊管理功能、連結網際網路、收發電子郵件、能與其它資訊產品進行資料同步或交換
輸入方式	觸控式、按鍵式、語音輸入或其它方式
處理器與作業系統	具備多工嵌入式微處理器與作業系統

2.2 iOS 作業系統

iOS 是由蘋果電腦公司(Apple Computer, Inc.)為 iPhone 所開發的作業系統，後來涵蓋範圍延伸至 iPod touch、iPad 及 Apple TV 等裝置上。如同 Mac OS X 作業系統一樣，也是以 Darwin 來做為基礎的。iOS 的系統架構層次分為四個：核心作業系統層（the Core OS layer），核心服務層（the Core Services layer），媒體層（the Media layer），觸控應用層（the Cocoa Touch layer）**[5]**。如圖 3

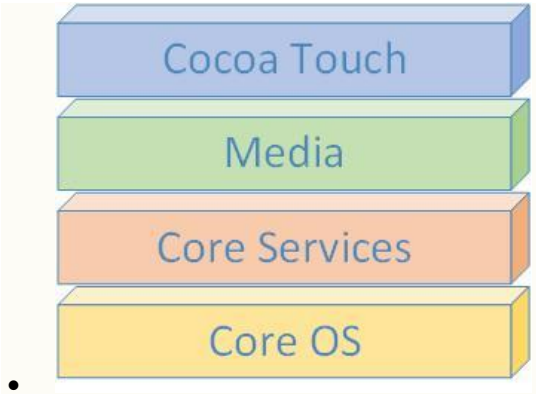

圖 3 iOS 四層架構

2.3 iPhone Configuration Utility

iPhone Configuration Utility(iPhone 設定工具程式,iPCU)能製作、維護、加密和安裝設定描述檔，追蹤和安裝配置描述檔與授權的應用程式，並且擷取裝置的資訊（包含控制台記錄）。
設定描述檔是 XML 格式檔案，含有裝置安全性規則與限制、VPN 設定資訊、Wi-Fi 設定、電子郵件和行事曆帳號，並允許 iPhone、iPod touch 和 iPad 與企業系統搭配使用的認證憑證。設定描述檔能快速把設定和授權資訊載入到裝置上**[6]**。

2.4 SCAP

Security Content Automation Protocol（安全內容自動化協定），目的為自動化弱點管理與標準化。結合開放性的標準，列舉出軟體的弱點漏洞與不適宜或錯誤的配置等相關的問題，用於協助找出漏洞，並提供方法及量測和量度這些調查出來的結果，用來評估相關弱點漏洞可能產生的影響**[9]**。

2.5 OVAL

Open Vulnerability and Assessment Language 開放性漏洞和評估描述語言，是一種國際性、資訊安全、社群標準以促進開放及公開的安全性內容，標準化跨越安全性工具及服務範圍整個資訊的轉移過程，OVAL 規範三個主要評鑑過程的步驟：描述系統設定訊息用來進行測試、分析系統指出機器狀態，如漏洞、組態、修補程式狀態等、及報告評鑑的結果，OVAL 是 IT 漏洞的彙集公開與內容來公開的使用語言**[9]**。

2.6 NVD

National Vulnerability Database 美國國家漏洞資料庫，遵循美國聯邦資訊安全法(Federal Information Security Management Act，簡稱 FISMA)

的要求，由美國國土安全部的國家網路安全辦公室資助，美國國家標準與技術研究院電腦安全部門之資訊技術實驗室負責建置，主要提供美國政府存放資訊安全漏洞標準化管理的資料庫。提供許多政府單位透過 SCAP (Security Content Automation Protocol)協定使用安全自動化的漏洞管理和安全檢測的機制並且評鑑風險，存放 SCAP 所使用到的共用標準相關資料儲藏資料庫，採用 CVE (Common Vulnerabilities Exposures)編號來作為資訊安全漏洞識別的依據**[9]**。

2.7 XCCDF

Extensible Configuration Checklist Description Format 可擴展設定配置清單描述格式，為一組特定語言提供撰寫安全檢查表、測試基準和相關的各種文件，進而促使更廣泛地應用在優良的安全實作上。XCCDF 文件包含描述對於目的系統以結構化的方式收集安全性的設定組態規則，所規範目的是支援資訊之交換、文件檔產生、組織及情境安排、自動化一致性的測試、一致性之評分，XCCDF 同時定義了一個資料模型與格式，用來儲存一致性的測試結果**[9]**。

2.8 CVSS

Common Vulnerability Scoring System 通用弱點評估系統，是由 FIRST 和 CVSS-SIG 共同發布的，目前版本為 CVSS v2.0，提供一個開放性的架構與使用開放和標準化的方法評分 IT 漏洞，現在已經成為美國聯邦政府的安全內容自動化協定(SCAP)的一個標準，用於標準化與自動化的弱點漏洞管理，CVSS 會以 Base、Temporal、Environmental 三個度量當作評分的方向，在每一個度量都有相關的評量項目，在 Base 的度量共提供 6 項評量項目，如存取的路徑、攻擊的複雜度等，NVD 只有提供 CVSS v2.0 Base 的度量在弱點漏洞資訊的提供上，而風險等級的區分範圍依照 CVSS v2.0 Base 的評分標準，分別為低(Low):0.0 到 3.9、中(Medium):4.0 到 6.9、高(High):7.0 到 10.0**[9]**。三個度量評分項目如圖 4 所示**[3]**。

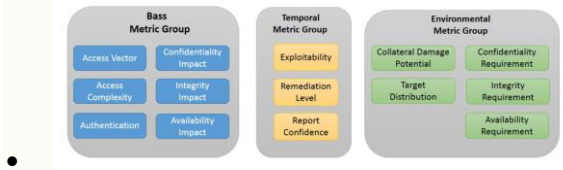

圖 4. CVSS 公制組

2.9 XML

Extensible Markup Language 可擴展標記語言，由 W3C 於 1996 年底提出的標準，在 1998 年 W3C 正式通過推薦 XML 1.0 版，是從 SGML 衍生出來的簡化格式，屬於 meta-language 的一種，可以用來定義任何一種新的標示語言，XML 的制定是為了改善 HTML 無法自訂標籤及只能應用在顯示資料的缺點，因此 XML 更適合處理各類複雜的文件與在網路上交換資料。XML 除去了 SGML 複雜且少用的規則，讓使用者有彈性的定義屬於自己的文件型態，因此 XML 具有結構化、可擴展、自我描述等特性，搭配排版樣本文件可以做到顯示的效果，所以弱點資料庫大多使用此格式類型來做資料交換的優先選擇**[1]**。

3. 系統架構

行動裝置設備應用愈來愈廣泛，企業單位也會配發行動裝置給相關人員。從資訊單位角度而言，如何管理行動裝置相關設定和使用軟體以不至於產生資訊安全問題，便是一項重要課題。本研究依循 SCAP 安全自動化協定(Security Content Automation Protocol)標準之一的可擴展設定配置清單描述格式(Extensible Configuration Checklist Description Format，XCCDF)，提供一個對於 iOS 行動裝置配置設定檔檢測的平台。使用蘋果電腦公司(Apple Computer, Inc.)的 iPCU 工具 (iPhone Configuration Utility)製作符合企業資訊安全政策的行動裝置配置檔，透過本系統來輔助檢測是否符合美國國家安全局(National Security Agency，NSA)安全配置建議(Security Configuration Recommendations)，系統能讓使用者在線上或者下載觀看檢測報告，評分部份透過分數說明，能讓使用者瞭解現行配置檔的安全程度。系統也提供線上配置檔維護功能，使用者能選擇是否參照系統所提供的配置建議設定；或是自行維護配置檔，透過這兩種方式都能立即在線上觀看維護後的報告結果。檢測系統流程如圖 5 所示。

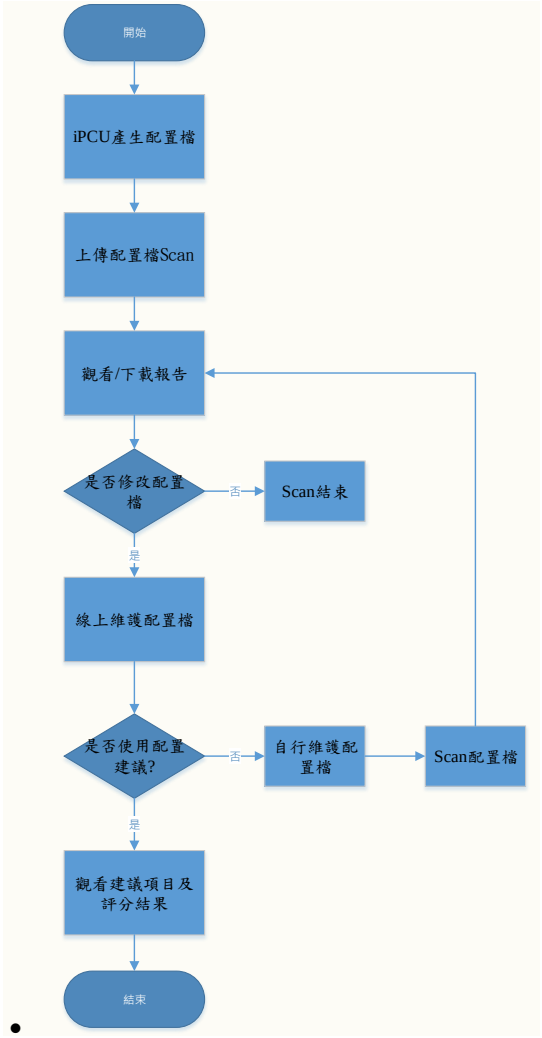

圖 5. 檢測系統流程圖

4. 系統開發實作

本研究依循 SCAP/XCCDF 裝置設定檢查為研究開發方向，依據美國國家安全局(National Security Agency)所發佈的配置設定建議**[8]**，搭配第三方軟體套件 jOVAL**[7]**，於 Ubuntu 作業系統上使用 JSP 網頁技術實作出行動裝置配置檔檢測網站，針對 iPhone 裝置設定檔做檢測，並提供檢測結果報告參考及線上維護配置檔功能。表 2 為檢測系統的開發環境和使用工具。

表 2 系統開發環境和工具

作業系統	Ubuntu Linux
開發工具	Java SE Development Kit(JDK)6 Eclipse JUNO
程式語言	JavaServer Pages(JSP) JavaScript
測試環境	Mozilla FireFox Web Browser Eclipse External Browser

圖 6 行動裝置配置檔檢測首頁

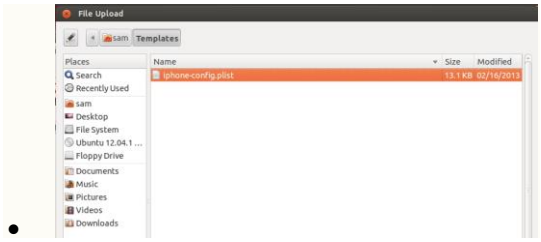

圖 7 選擇檢測配置檔

圖 8 選擇檢測配置檔

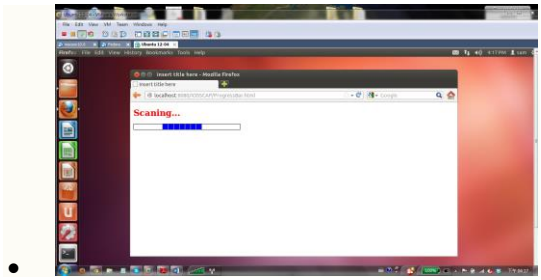

圖 9 配置檔檢測掃瞄中

圖 10 配置檔檢測掃瞄完成，點選 GO 回檢測首頁

圖 11 線上觀看檢測結果報告

圖 12 配置檔維護，手動或系統配置建議

圖 13 使用系統配置建議

圖 14 不使用配置建議，手動修改

5. 結論

Apple iOS 是一個發展快速、普及率遽增的智慧型手機作業系統，有著讓使用者自行擴充軟體的功能，所以也比傳統手機更令人依賴。

本研究是對於行動裝置的配置設定提出一套檢核測試方法及其安全性的改善，因此針對 Apple iPhone 智慧型手機，在不進行 Jailbreak 情況下搭配第三方軟體套件所開發的檢測平台，對於 iPhone 配置設定檔以離線方式做檢測掃瞄，期望以後能朝向使用 APP 的方式來做 iPhone 內部檢核測試。

致謝

本研究部分成果承蒙國科會計畫經費補助(NSC 101-2221-E-017-013)，特此致謝。

參考文獻

[1] A. Blyth, An XML-based architecture to perform data integration and data unification in vulnerability assessments, Information Security Technical Report, 8(4), pp.14-25, 2003.

[2] Android and iOS Combine for 91.1% of the Worldwide Smartphone OS Market in 4Q12 and 87.6% for the Year, According to IDC, http://www.idc.com/getdoc.jsp?containerId=prUS23946013#.UUWA5hwRIpw.

[3] CVSS v2 Complete Documentation, http://www.first.org/cvss/cvss-guide.html.

[4] D. C. Harrill and R. P. Mislan, A small scale digital device forensics ontology. Small Scale Digital Device Forensics Journal, 1(1), pp.242, 2007.

[5] iOS Technology Overview, http://developer.apple.com/library/ios/#documentation/miscellaneous/conceptual/iphoneostechoverview/Introduction/Introduction.html.

[6] iPhone Configuration Utility, http://help.apple.com/iosdeployment-ipcu/win/1.2/?lang=en-us.

[7] jOVAL, http://joval.org/.

[8] National Security Agency Central Security Service, http://www.nsa.gov/ia/mitigation_guidance/security_configuration_guides/operating_systems.shtml .

[9] National Vulnerability Database.(NVD).(2008). http://nvd.nist.gov/, May, 2008.

[10] S. G. Punja and R. P. Mislan, Mobile Device Analysis. Small Scale Digital Device Forensics Journal, 2(1), pp.1-16, 2008.