Android 平台智慧型行動裝置管理系統設計與實現

Design and implementation of a mobile device management system on android platform

張世奇
國立高雄師範大學　資訊教育研究所
47go.tw@gmail.com

楊中皇
國立高雄師範大學　軟體工程與管理系
chyang@nknu.edu.tw

***摘要*—本研究設計並實作一個網頁式(web-based)的行動裝置管理系統(Mobile Device Management, MDM)。隨著國人使用智慧型裝置的普及，因此許多企業允許員工自攜裝置(Bring-Your-Own-Device, BYOD)的趨勢越來越明顯，但隨之而來的資訊安全風險也日益增加，如何取得資訊安全與方便性的平衡，是目前企業所面臨的資訊安全管理問題。本研究運用 Android SDK 並配合網站伺服器進行行動裝置的管理，並實作「SCAP 安全分數掃描」、「應用程式 APK 檔驗證」兩個功能模組，掃描裝置上是否安裝有雜湊值不符的應用程式與取得安全性評估分數，供管理者評估是否開放該行動裝置存取公司資料。本系統協助管理人員針對不同情況，對 Android 行動裝置進行遠端管理，並於伺服端提供可跨平台操作的介面與安全性評估報告，以提升管理設備的效率。**

***關鍵詞*—自攜裝置, 行動裝置管理, 安全內容自動化協定, 雜湊函數**

***Abstract*—This paper presents the design and implementation of a web-based mobile device management (MDM) system. The usage of mobile devices has become increasingly popular so that many enterprises provide BYOD (Bring-Your-Own-Device) policy to their employees. When the trend of applying BYOD policy is becoming evident, the information security threats are also increasing. How to balance the convenience and the information security impacts is a major information security management problem for enterprises. By integrating Android APIs, the Security Content Automation Protocol (SCAP) and APK file integrity check, we have developed a MDM system that enables managers to scan mobile devices belong to employees, obtain a security evaluation score and verify the integrity of APK files. As a result, the evaluation reports for BYOD devices can be produced and the managers can block devices with security concerns based on those reports. The system can assist administrator to manage Android mobile devices from remote site more efficiently, and provide a more secure environment for BYOD scenarios.**

***Index Terms*—BYOD, Mobile Device Management, SCAP, Hash Functions**

一、前言

隨著資訊科技技術的進步以及無線網路的普及，現今行動裝置的運算、可攜性與便利性已可滿足處理簡易的事務，因此帶動了企業的行動化應用，並形成員工自攜裝置的浪潮。

企業讓員工自攜裝置來上班，有其優缺點。優點是員工使用自己熟悉的電腦或行動裝置來工作，可以提升工作的效率。但是缺點則是資訊安全控管的問題，試想如果公司商業機密被員工不當使用或是外洩，或者員工不小心將行動裝置

遺失了，而設備上存放著公司重要的機密或交易相關資訊，那就會造成公司很大的損失。另一方面，因為這些行動裝置有非常多種的型號、類型、韌體，以及作業系統[9]等，所以企業得要面臨多種設備存取企業系統的挑戰。

市場上有不少的行動裝置管理系統之產品，但其功能大多類似，例如：設備規則配置、應用程式管理、韌體更新[9]、安全管理、資產管理、服務管理等管理功能，鮮少有提供行動裝置組態的安全分數掃描和應用程式APK檔雜湊值驗證。在企業開放 BYOD 的浪潮下，如果能提供企業一個快速判斷是否可讓該行動裝置存取企業內部資料的準則，將可以減少企業開放 BYOD 後產生的管理問題。

本研究針對上述的問題，提出解決的方法，設計與實作一套能有效協助管理企業內部行動裝置的管理系統。透過 Android SDK 提供的 API 將裝置內的相關組態值傳送到支援安全內容自動化協定(Security Content Automation Protocol, SCAP)的 Server 上進行掃描，以得到安全分數與測試報告，並對裝置內所安裝的應用程式進行雜湊值運算，進而作為是否開放該行動裝置存取企業內部資料的依據。

二、文獻探討

(一) 自攜裝置(Bring your own device, BYOD)

BYOD 是行動運算普及後的一種現象，在企業裡有不斷增長的趨勢，員工拿個人的行動裝置連接到公司的網路來存取企業的資訊和進行一些日常的商業行為。BYOD 有許多的優點，包含提高工作生產效率、提高員工工作滿意度，因為不受時間和地點影響，使員工可以快速取得公司內部資訊，提升資訊處理速度，相對也就提升工作效率[7]。根據 Cisco 於 2012 年做的一項調查顯示，約有 600 家公司允許員工使用個人設備來工作。Dell 公司也進行了調查，結果發現，開放 BYOD 政策的公司其員工生產力都增加了 74%以上，調查的結果更促進企業採用開放 BYOD 政策來增加生產力[8]。

相對於 BYOD 的許多優點，企業中也因此產生了新的管理問題。企業 IT 需要解決多種行動裝置作業系統和相關的安全問題[7]，例如行動裝置上有公司的重要商業機密或交易資料，但員工不小心遺失這個設備，或者員工離職，造成未經授權的使用者讀取公司資料，此外，設備損壞、病毒攻擊等等狀況都會造成公司很大的損失，所以 BYOD 的管理問題也是目前企業面臨的安全問題之一。

對這些行動裝置採取安全管理政策可以保護公司的資料，但安全政策要完全套用至員工個人的行動裝置上難度之高，這是一個關鍵因素。這就是開放 BYOD 後公司將產生多種的潛在安全問題的原因。資料一旦進到不被公司控制的裝置上時，該資料也等同於不再受到控制了[6]。隨著 BYOD 越形普及，企業的管理者更需要確定是否開放 BYOD。

BYOD 的安全模組功能

針對 BYOD，目前有三個主要的安全模組，分別為行動裝置管理(Mobile Device Manager, MDM)、行動應用程式管理(Mobile Application

Management, MAM)、行動資訊管理(Mobile Information Management, MIM)三種[4]。這些安全模組根據行動裝置與存取資料的使用型態分為四類基本的解決方案[4]：使用者存取控制和裝置辨識、資料監控和保護、行動應用程式安全和完整與承諾(Compliance)。以上四類解決方案，只是基本的安全要求，並無法完全滿足越來越多樣化的進階攻擊手法。Eslahi et al(2014)提到 Google Play、Apple Store 和 Windows Store 等這類應用程式商店，提供使用者隨意搜尋與下載應用程式的便利性，但對於應用程式的安全顧慮，這些商店僅針對病毒或惡意軟體等常見的應用程式進行處理，並沒有檢查一個應用程式是否符合企業的特定安全政策。因此他提出了一個 secure metamarket (SMM) 系統，其目的是確保安裝在個人行動裝置上的應用程式符合企業的安全政策。而 Chang et al(2014)提到了一種在作業系統裡，利用虛擬化技術，將企業空間和個人空間區分開來的分離技術(Separation Techniques)，可防止在企業空間的作業影響到個人空間的隱私或資料，也可防止個人空間的操作影響到企業

空間資料。

(二) 行動裝置管理(Mobile Device Manager, MDM)

行動裝置管理(Mobile Device Management 簡稱為 MDM)是一種提供企業針對組織內的行動裝置進行管理的一種管理系統。

MDM 運用無線通訊技術(例如:Over-the-Air (OTA) or Wi-Fi)進行遠端的行動裝置管理，能監控裝置的狀態，並控制裝置的功能[5]。MDM 主要是由 MDM Agent 和 MDM Server 兩個部分組成[4]

MDM Agent

安裝在行動裝置上的一個應用程式，其主要目的是用來傳送行動裝置上的資料(例如：裝置型號、狀態、位置等)給其 MDM Server，並在行動裝置上執行一些由管理者在 MDM Server 上設定的安全政策和其它的裝置管理設定，如限制行動裝置不能使用照相機、密碼政策強度與遠端進行資料抹除等。

MDM Server

主要用來接收由 MDM Agent 傳送過來的資料，並根據管理者設定的安全政策和操作，相對應的去觸發那些受管理的行動裝置，讓行動裝置上的 MDM Agent 執行相關的命令[4]。

(三) SCAP

安全內容自動化協定(Security Content Automation Protocol, SCAP)由美國國家標準技術研究院(National Institute of Standards and Technology, NIST)所提出，目的為結合開放性的標準來自動化與標準化弱點的管理。是目前美國較成熟的資訊安全評估標準[1]。

(四) 單向雜湊函數

單向雜湊函數又稱訊息摘要(Message Digest)演算法，擁有不可逆的特性，將任意長度的資料經過單向雜湊函數的運算後，可得到一個固定長度的雜湊值，並且無法再透過該雜湊值來反推原始資料。因此，單向雜湊函數適合用來驗證資料的完整性(Data Integrity)，以確定資料是否有遭到修改。

目前常見的雜湊函數有 MD5、SHA-1、SHA-256 等。訊息摘要的長度決定了雜湊函數的安全程度。MD5 的輸出摘要長度為 128 位元，而 SHA-1 的輸出摘要長度為 160 位元，兩者的安全程度皆有疑慮，而訊息摘要的長度越長，雖然較為安全，但相對的執行速度也會較慢。本研究採用美國國家標準技術局(NIST)於 2002 年公佈的 FIPS 180-2 中之 SHA 256 雜湊函數演算法[2]，對行動裝置端的應用程式 APK 檔進行雜湊運算，並將運算結果傳至伺服端進行比對，以判斷行動裝置端安裝的應用程式 APK 檔是否有遭受到竄改。

表一 常見單向雜湊函數的比較

項目	MD5	SHA-1	SHA-256
摘要長度(位元組)	16	20	32
安全性	不安全	有疑慮	2128
標準公佈年份	1992	1995	2002

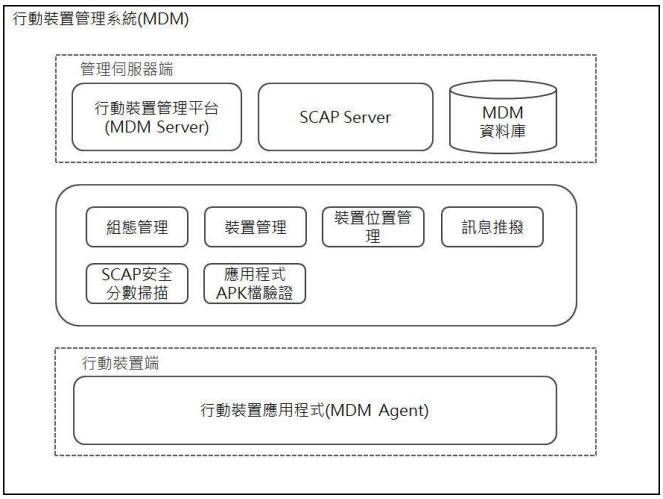
三、行動裝置管理系統設計與實作

(一) 系統架構設計

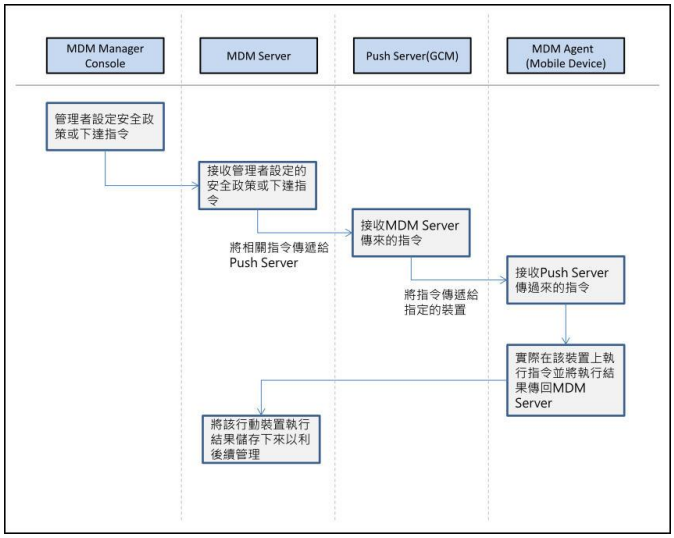
本研究設計並實作 Android 平台行動裝置管理系統。系統架構分管理伺服端與行動裝置端，管理伺服端包含「行動裝置管理平台」、「SCAP Server」與「MDM 資料庫」，「MDM 資料庫」用來存放行動裝置傳送過來的資料，如裝置座標。行動裝置端為「行動裝置應用程式」。提供之功能模組包含「組態管理」、「裝置管理」、「裝置位置管理」與「訊息推撥」。除了實作一般行動裝置管理系統常有的功能模組外，亦考量現今 BYOD 的應用場域大多為企業，系統如果能提供裝置組態設定值的安全評分，作為是否開放該行動裝置 BYOD 政策的一項依據，將能提升安全性與管理上的效率。此外員工自攜裝置存取公司資料，亦需考量裝置是否安裝有安全疑慮的應用程式，以防資訊安全漏洞。綜合上述，本研究實作 MDM 系統並建置「SCAP 安全分數掃描」與

「應用程式 APK 檔驗證」兩個模組，提升企業採用 BYOD 的安全管理效率，系統之架構如圖一所示。「SCAP 安全分數掃描」模組用來進行裝置內組態設定值的安全分數掃描，以得到安全分數與測試報告，藉以作為是否開放該行動裝置 BYOD 政策的依據。「應用程式 APK 檔驗證」模組用來進行應用程式 APK 檔的雜湊值驗證，藉由比對行動裝置端的應用程式 APK 檔與管理者上傳的 APK 檔之雜湊值，判斷行動裝置端上所安裝的應用程式是否有經過竄改，並且支援遠端移除應用程式。

管理者透過 MDM Manager Console 在 MDM Server 上設定安全政策或進行其它的操作，MDM Server 將管理者所設定的相關指令，透過 Google 雲端通訊(Google Cloud Messaging, GCM)服務，傳送到受管理行動裝置上的 MDM Agent，MDM Agent 接收到指令後，即對該行動裝置進行實際的政策設定或執行指令。MDM Agent 能發送該裝置軟硬體資訊及定位座標至 MDM Server，MDM Server 與 MDM Agent 之間的溝通程序，如圖二所示。



圖一 系統架構圖



圖二 系統元件交互圖

(二) 系統實作

本研究 MDM Agent 使用 Eclipse 整合式開發環境搭配 Android SDK 進行開發。MDM Server 使用 Apache、MySQL 和 PHP 來進行開發，並透過 GCM 服務實現指令的推撥。「組態管理」模組透過 Android SDK 的 DevicePolicyManager 類別實作，包含是否可以使用照相機功能、密碼強度與遠端清除資料。「裝置管理」模組透過 Build 與 WifiManager 等類別實作，進行關閉裝置 Wifi 與裝置鎖定。「裝置位置管理」模組使用 LocationManager 等類別來取得裝置目前的位置資訊。「訊息推撥」模組透過 GCM 服務進行訊息發送。「SCAP 安全分數掃描」實作的方法是將行動裝置內的組態設定值，運用 HTTP POST 的方式傳給系統，系統中的 SCAP 服務接收到行動裝置的組態設定值後，進行安全分數的估算，並把安全分數與測試報告傳至 MDM Server 上保存供後續管理之用。「應用程式 APK 檔驗證」實作的方法分成行動裝置端和伺服端。首先，行動裝置端是利用 Android SDK 的 MessageDigest 類別對裝置內的應用程式 APK 檔進行運算，以取得 SHA-256 雜湊值，接著將這些應用程式 APK 檔的雜湊值透過 HTTP POST 的方式傳遞到 MDM Server 裡進行保存。伺服端使用 OpenSSL 提供的雜湊函式，針對由管理者上傳的應用程式 APK 檔進行運算所取得的 SHA-256 雜湊值，並將取得的雜湊值保存在 MDM Server 裡。MDM Server

會列出由行動裝置端所上傳的應用程式和其雜湊值，並且與管理者上傳的應用程式 APK 檔雜湊值進行比對。若比對結果不一樣，代表該行動裝置上所安裝的應用程式可能遭受竄改，此時管理者可以透過管理介面提供的遠端移除功能，移除該行動裝置上的應用程式。

四、行動裝置管理系統

(一) MDM Agent

本研究之行動裝置管理系統 MDM Agent 的使用介面有提供「傳送裝置位置」、「傳送裝置配置檔到 SCAP Server」、「取得 SCAP 安全分數」、「應用程式 APK 檔雜湊運算」等功能，如圖三所示。

(二) MDM Server

本研究之行動裝置管理系統 MDM Server 的管理介面，在「裝置管理」頁面裡會顯示出受本管理系統所管理的行動裝置清單，在清單中列出行動裝置的裝置型號、作業系統版本與安全分數等欄位資料，並且提供「鎖定」該行動裝置的功能，及推撥訊息等功能，如圖四所示。

圖三 MDM Agent 使用介面

圖四 MDM Server 管理介面

SCAP 安全分數掃描

在 MDM Agent 上點「傳送裝置配置檔到 SCAP Server」鈕，即會將該行動裝置上的組態設定值傳送到 SCAP 的 Server 上進行掃描，並將掃描結果的安全分數與測試報告傳送到 MDM Server 上進行保存，如圖五、圖六所示。

圖五 MDM Server 保存掃描結果之安全分數

圖六 SCAP 安全分數掃描結果之測試報告

應用程式 APK 檔驗證

在 MDM Agent 上點「應用程式 APK 檔雜湊運算」鈕，即會在背景進行該行動裝置上的應用程式 APK 檔 SHA-256 運算，並將運算產出的雜湊值傳遞到 MDM Server 上進行管理，如圖七所示，當系統比對該應用程式雜湊值與管理者所上

傳的應用程式雜湊值不同時，即會用紅色文字來標示錯誤的雜湊值並顯示正確的雜湊值，而在管理的那個欄位中，提供解除安裝的功能，進而要求行動裝置端移除該應用程式。

圖七 應用程式 APK 檔驗證之管理介面

五、結論

企業開放 BYOD 政策，帶來了不少的優點，但隨之而來的管理問題也是企業所要改善處理的課題。本研究所設計與實作之行動裝置管理系統具備 SCAP 安全分數掃描、應用程式 APK 檔驗證等功能模組，能更符合企業採用 BYOD 的安全需求。當行動裝置要存取公司內部資料時，必須先加入到行動裝置管理系統的管理名單內，管理者可透過系統的安全政策管理功能進行相關的政策配置，如是否可以使用照相機、密碼強度等，要求受管理的行動裝置必須同步公司的相關安全政策。當行動裝置遺失或被盜時，可以透過裝置位置管理功能提供的管理介面，進行找尋或命令行動裝置發出警報聲，以提高裝置的尋獲率。SCAP 安全分數掃描功能，提供了安全分數與測試報告，讓企業管理者迅速判斷是否該開放這台行動裝置存取公司內部資料。最後，應用程式 APK 檔驗證功能提供了驗證行動裝置端上所安裝的應用程式 APK 檔是否有遭受竄改。

本管理系統能協助企業內管理人員針對不同情況下，對 Android 的行動裝置進行遠端控制，並於伺服端提供可跨平台操作的介面與安全分數的檢視報表，以提升管理人員管理設備上的工作效率。在建構本行動裝置管理系統的過程中，亦有幾項問題有待解決，像如何有效地區分行動裝置上個人環境與工作環境，防止員工加入 BYOD 後，個人隱私資料被 MDM 系統讀取的問題。

六、參考文獻

[1] 郭政良、楊中皇，”Android 行動裝置組態管理系統的設計與實現”，第二十五屆全國資訊安全會議(CISC 2015)，高雄第一科技大學，2015 年 5 月。

[2] 楊中皇，”網路安全理論與實務”，學貫行銷股份有限公司，2008。

[3] J. M. Chang, H. Pao-Chung, and C. Teng-Chang, "Securing BYOD," IT Professional, Vol. 16, pp. 9-11, 2014.

[4] M. Eslahi, M. V. Naseri, H. Hashim, N. M. Tahir, and E. H. M. Saad, "BYOD: Current state and security challenges," in Computer Applications and Industrial Electronics (ISCAIE), 2014 IEEE Symposium on, pp. 189-192, 2014.

[5] Keunwoo Rhee, Woongryul Jeon, and d. Dongho Won, "Security Requirements of a Mobile Device Management System," International Journal of Security & Its Applications, Vol. 6, pp. 353-358, April 2012.

[6] K. W. Miller, J. Voas, and G. F. Hurlburt, "BYOD: Security and Privacy Considerations," IT Professional, Vol. 14, pp. 53-55, 2012.

[7] A. Scarfo, "New Security Perspectives around BYOD," Broadband, Wireless Computing, Communication and Applications (BWCCA), 2012 Seventh International Conference on, pp. 446-451, 2012.

[8] M. R. Waterfill and C. A. Dilworth, "BYOD: Where the Employee and the Enterprise Intersect," Employee Relations Law Journal, Vol. 40, pp. 26-36, 2014.

[9] L. Liu, R. Moulic, and D. Shea, "Cloud Service Portal for Mobile Device Management," e-Business Engineering (ICEBE), 2010 IEEE 7th International Conference on, pp. 474-478, 2010.