モバイル端末のリスク分析と対策の自動適用手法

陳 帥*† 金岡 晃*‡ 松尾 真一郎 ‡ 加藤 雅彦* § 須賀 祐治 §
岡本 栄司 †

† 筑波大学
305-8573 茨城県つくば市天王台 1-1-1
chen@cipher.risk.tsukuba.ac.jp*
okamoto@risk.tsukuba.ac.jp

‡ 情報通信研究機構
184-8795 東京都小金井市貫井北町 4-2-1
akira.kanaoka@is.sci.toho-u.ac.jp*
smatsuo@nict.go.jp

§ 株式会社 インターネットイニシアティブ
101-0051 東京都千代田区神田神保町 1-105
masa@iij.ad.jp*
suga@iij.ad.jp

あらまし スマートフォンを業務に利用する場合，その管理が大きな問題となる。現状，MDM（モバイルデバイスマネジメント）としてシステムが提供されているが，スマートフォンの業務利用に関するリスクの判断は MDM システムの運用者や組織の意思決定者が行わなければならない。本論文ではスマートフォンのリスク評価をスマートフォンの状況に応じて行いリスクに応じた MDM システムによる動的な管理と残存リスクの提示を可能にする仕組みを提案し，そのプロトタイプを Apple 社の iOS に対応した MDM システムとして開発した。

Real-time Risk Analysis and Automatic Configuration for Mobile Devices

Shuai Chen*† Akira Kanaoka*‡ Shin'ichiro Matsuo‡ Masahiko Katoh*§
Yuji Suga§ Eiji Okamoto†

†University of Tsukuba
1-1-1 Tennodai, Tsukuba, Ibaraki 305-8573, Japan
‡National Institute of Information and Communications Technology
4-2-1 Nukui-Kitamachi, Koganei, Tokyo 184-8795, Japan
§Internet Initiative Japan Inc.
1-105 Kanda Jinbo-cho, Chiyoda-ku, Tokyo, 101-0051, Japan

Abstract Smartphones have been widely deployed for business purposes these years. It used to be complicated for IT administrators in large organizations to manage all the smartphones until MDM (Mobile Device Management) was introduced. However, when the environment changes, MDM system alone cannot deal with the unknown risks in real-time without administrators' interaction. In this paper, we propose a new system combined the MDM system with a risk analysis system, which can analyze and visualize smartphones' environmental risks dynamically and help MDM system to configure smartphones automatically. In addition, it can output the remaining risks after configuration profiles been installed by the smartphones. We also developed a prototype system, which supports Apple's iOS devices.

1 Introduction

Mobile devices are becoming more and more powerful these years. The computing resources of them are almost the same level as PCs. In addition to the computing resources, mobile devices have thus rich sensors like camera, gyro, accelerometer that make them very popular for business purposes. The usage of mobile devices in business can be divided into 2 types: one is to use private mobile devices of employees for business purposes, named BYOD (Bring Your Own Device). And the other one is to use mobile devices lent by a company to employees for private purposes.

On the other hand, the convenient features of mobile devices also bring many unknown risks, which are quite different from those exist on PCs. It used to be a difficult problem for deploying and managing mobile devices for business purposes until MDM was introduced.

MDM is short for Mobile Device Management, which gives organizations the ability to securely enroll mobile devices, wirelessly configure and update settings, monitor compliance with corporate policies, and even remotely lock or wipe managed devices without users' interaction. If some settings or security policies have been changed, the administrators only need to configure the settings on the server, all the devices managed by the server will be updated automatically and most of the time silently. It is that simple.

However, the problem still exists. Risks may be affected by the external conditions. For example, when a user brings his smartphone to a bar and wants to access the confidential contents inside his company, the security setting for the usage inside the company should apparently not be enough. The environment has changed, everything between the user's smartphone and the server inside the organization may be dangerous. If any of these risks have not been handled properly, the consequences may be disastrous. So what can the user do? Call the administrator to let him analyze the risks and change the settings. This is not a good method. Try to image the same episode in a large company. Thousands of employees will call the administrators just because they get out of the offices. This can drive the administrators crazy. In short, for those organizations which would like to deploy and manage mobile devices for business purposes conveniently and securely, the traditional risk management methods must be reconsidered. And MDM alone is indeed not enough at all. What we need is a system which can reduce the workload of the administrators, automate the entire process from risk analysis to the settings update, and should not be constrained by the platforms.

In this paper, we firstly propose a new framework of the MDM system, which contains risk analysis module to achieves risk analysis and automatic configuration generation based on the context provided by the administrators. And, the new system can feedback the remaining risks, which we believe is a very important concept but often be ignored during the management in fact. Then we develop a prototype system, which supports Apple's iOS devices to verify our theory.

2 Related Works

2.1 Apple iOS

Apple has its own mobile device management scheme. In this scheme, a XML-formatted document called Configuration Profile is used to make restrictions and change settings of the password policy, WiFi, VPN, etc. The scheme has a server system named MDM server which can push configuration profiles to iOS devices. Enterprise can either deploy its own MDM server or outsource one. However, the iOS devices do not communicate to the MDM server directly to get push notifications sent by the MDM server. Instead, Apple uses its own Apple Push Notification server (APNs) to send notifications to the iOS devices.

2.2 Google Android OS

Android OS does not have its own management scheme. However, thanks to the high flexibility of Android, various MDM scheme can be deployed to manage Android devices. For example, Android supports Microsoft Exchange Server which can be used as a MDM system. Third-party organizations or companies can provide MDM service using their original MDM systems and agent applications for Android devices.

2.3 Academic Studies

There are several academic studies discussing management of mobile devices[1, 2, 3, 4, 5, 6, 7, 8]. However, remaining risks feedback and automatic generation of configuration have not been discussed in these studies.

3 Proposed System

3.1 Shortcomings of the Conventional MDM Systems

As we mentioned before, though conventional MDM systems automate almost most of the administrator's work, it is still not enough. We summarize the shortcomings of the conventional MDM systems as follows:

- MDM alone can not deal with risks, especially environmental risks in real time. For most organizations, the security settings for mobile devices have to be changed with the environment. When the user gets outside the organization, the password policy should be more strict. But it's not quite convenient for either users or administrators to change the security settings even with MDM.
- Administrator is still an important role during the management. Though with MDM, new settings and restrictions can be applied by the users' devices automatically. It must be the administrators to analyze the risks and make the change happen from the server side. Consider that security policy can be different from department to department, it is really not an easy task.

In order to deal with these shortcomings and to enhance the usability of the conventional MDM systems, we propose a new MDM system. This is not just an ordinary MDM system. It combines conventional MDM system with risk analysis system. This makes it not only can deal with the environmental change automatically, but also automate the whole process from end to end, thus free the administrators.

3.2 Framework

Figure 1 shows the architecture of our proposed system. The specific workflow is as follows:

1. First, user accesses the system with his mobile device to start the risk analysis. At the same time, the system collects some environmental information from the device, like the current network information, firmware version, installed applications list etc.
2. With the information system collected, the risk analysis module now can make countermeasures to deal with the risks. In this step, administrator can import some third-party knowledge bases as a reference. These

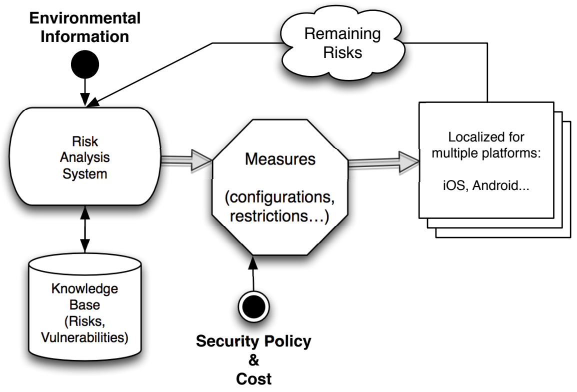

Environmental Information
Remaining Risks
Risk Analysis System
Measures
(configurations, restrictions...)
Localized for multiple platforms:
iOS, Android...
Knowledge Base (Risks, Vulnerabilities)
Security Policy & Cost

Fig 1: System architecture

knowledge bases contain the latest vulnerabilities and threat information.

3. At this stage, the output of the risk analysis module is just abstract countermeasure. To make it concrete, administrator must take into account some external factors of his organization, like the security policy and the cost which can be afforded. With these considerations, the countermeasures should become much more practical.

4. So far, the results are general, and not related to the specific platforms. The next step is to use the MDM system to protect the user's device. Since the specification of MDM differs with the platforms, administrators should localize the results retrieved from the risk analysis module for each platform respectively. For example, iOS uses configuration profiles to make configurations and restrictions, and Android often needs additional agent applications to change the settings.

5. Although MDM is becoming more and more powerful every year, it is impossible to handle all the risks alone in most cases. In our proposed system, we call those risks, which have been remained by the MDM module, the remaining risks. First, the MDM module would feedback the remaining risks to the administrators and the users. Based on the remaining risks, measures will be taken from both server and client sides. For example, change the firewall settings to cut off the communications or switch the service provided by the server to the limited edition.

4 Prototype System

In order to verify our proposed system, we developed a prototype system which supports Apple's iOS devices. It is a simple system and still in development, but it can explain our concept very well.

4.1 Functions

As Figure 2 shows, our prototype system consists of 3 main parts: the web interface, the risk analysis module combined with some third-party databases and the iOS MDM server. The specific processes are as follows:

- First, user accesses the prototype system with his mobile device (in this case, iPhone or iPad) via the web interface. The web

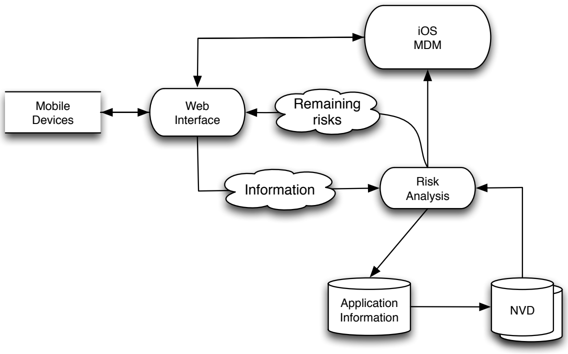
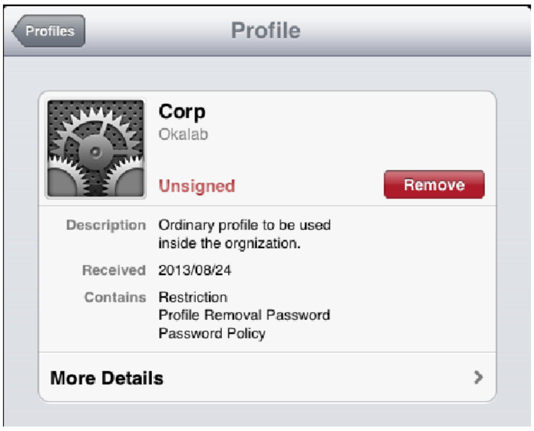


Fig 2: Prototype system overview



Corp
Okalab
Unsigned

Description: Ordinary profile to be used inside the orgnization.
Received: 2013/08/24
Contains: Restriction
Profile Removal Password
Password Policy

Fig 3: iOS configuration profile

interface is a simple web application. Meanwhile, environmental information will be collected from the target iPhone and the web application will send a command to the iOS MDM server to request for the list of installed applications on the target iPhone. Of course, there is a premise that the user's iPhone must be enrolled to the iOS MDM server of the prototype system in advance. Normally, the iOS MDM server will return the list to the web application.

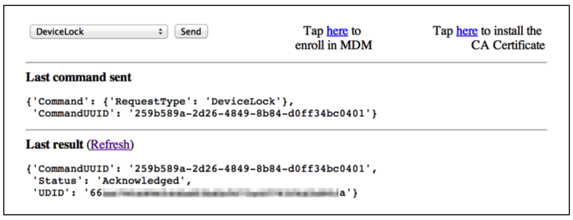
- After collecting the necessary information, the web application will then send these information to the risk analysis module to begin the risk analysis. In this prototype system, the risk analysis module has 2 functions: location-based configuration profile creation and installed applications vulnerabilities check.

  As we mentioned before, security settings should vary with location. For iOS, configuration profiles (a XML formatted document) are used to change settings and make restrictions (Fig 3). So in our prototype system, we prepared 3 kinds of configuration profiles for 3 different locations:

  – Organization Profile, which is for the users inside the organization. This profile contains the following settings:
    * Simple password allowed.
    * No data erase after entering the wrong passcode many times.
    * No applications or sensors will be prohibited, etc.

  – Domestic Profile, which is for the users outside of the organization but inside of Japan. This profile contains the following settings:
    * Normal password policy. Passcode length must be longer than 6, with at least one alphabet. All the data will be erased after trying the wrong passcode for 5 times.
    * No screen-shot allowed.
    * Backup of the device must be encrypted.
    * Prohibit the use of YouTube and FaceTime.
    * Proxy server and VPN settings, etc.

  – Foreign Profile, which is for the users outside of Japan. This profile contains the following settings:
    * The most stringent password policy. Easy passcode is not allowed. Passcode length is not less than 8, with at least one special character. All the data will be erased after trying the wrong passcode for 3 times.
    * Prohibit the access to the camera.
    * No screen-shot allowed.
    * Backup of the device must be encrypted.
    * Safari use with restrictions.
    * Proxy server and VPN settings, etc.


DeviceLock
Send
Tap here to enroll in MDM
Tap here to install the CA Certificate

Last command sent

```
{'Command': {'RequestType': 'DeviceLock'},
 'CommandUUID': '259b589a-2d26-4849-8b84-d0ff34bc0401'}
```

Last result (Refresh)

```
{'CommandUUID': '259b589a-2d26-4849-8b84-d0ff34bc0401',
 'Status': 'Acknowledged',
 'UDID': '66[redacted]a'}
```

Fig 4: Simple iOS MDM server

Though GPS is more accurate to determine the user's location, but the use of GPS may be prohibited by the configurations. So in our prototype system, we use IP address to determine the user's location.

Then the risk analysis module will check the installed applications list to find out whether there is any threat or vulnerability. We import NVD (National Vulnerability Databse) [9] to help us to accomplish this task. Along with the applications' names, the list also contains the applications' identities and version numbers. The risk analysis module will compare these information to the NVD database. If there is a vulnerability, the result will be sent back to the web interface to remind the user. This feedback is part of the remaining risks.

- The last part of the system is the iOS MDM server. Since Apple does not release the detail of the iOS MDM protocol publicly. We referred to David Schuetz's [11] white paper in Blackhat USA 2011. Based on his research and Apple's Configuration Profile Reference [10] (which describes the commands supported by iOS devices for MDM service), we developed a basic iOS MDM server with Python language, which is compatible with iOS 6.x devices. The iOS MDM server will push the configuration profiles to the target iPhone.

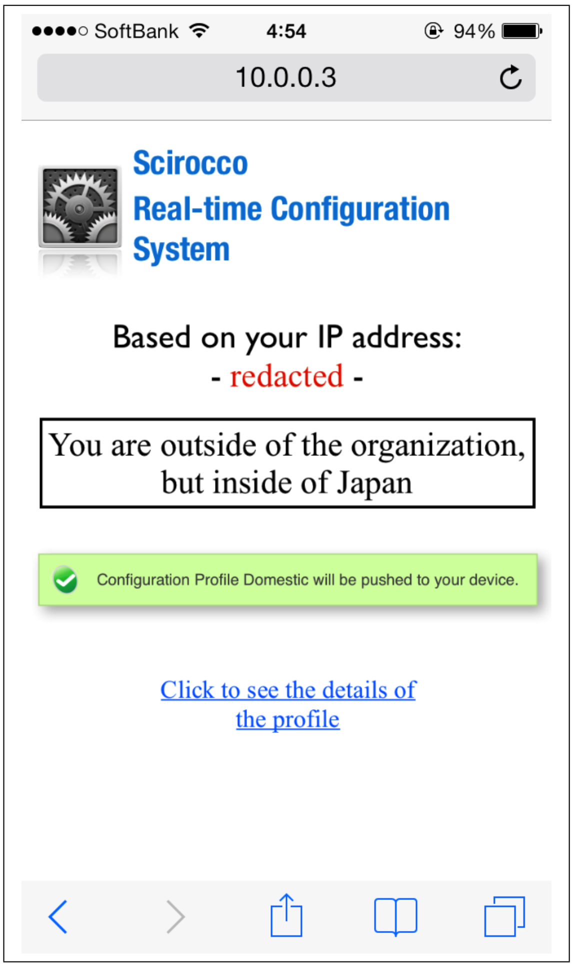
5 Experimental Result

To test our prototype system, we run the system on a 2012 Mac mini (OS X Server 2.2) with 2.5GHz intel dual-core core i5 processor and 4GB memory. Figure 4 shows the home screen of our simple iOS MDM server: users can enroll his iOS device to the MDM server directly from the page. After the enrollment, the system can start to test the target device. All the communications between the target device and the MDM server will be logged and can be confirmed from the MDM interface.

Figure 5 shows the web application of the prototype system. After launching the application, user's IP address and location information will be displayed on the screen automatically, and the corresponding configuration profile will be pushed to the user's device. No need for the user's interaction. All the configuration profiles are password protected, so the user can not remove the profile without the administrator's permission.

Figure 6 shows the applications vulnerabilities check function. Applications installed on the target device will be displayed on the screen alongside the version numbers. If potential threats exist in the installed applications, a warning message will be displayed to remind the user. In the prototype system, we only extract the application's name, identity and version number to compare to the third-party database. The database is customized from the NVD database. This function is still in development. We prepare to import more third-party databases and items to compare, such as CVSS [12] and JVN [13].

We take the 1st generation iPad with iOS 5.1.1 as the test device, and access the system to see the whole computation and response time. Since the key steps (get the installed applications list and push configuration profiles to the target device) need Apple's push notification service, the result is heavily influenced



Scirocco
Real-time Configuration System

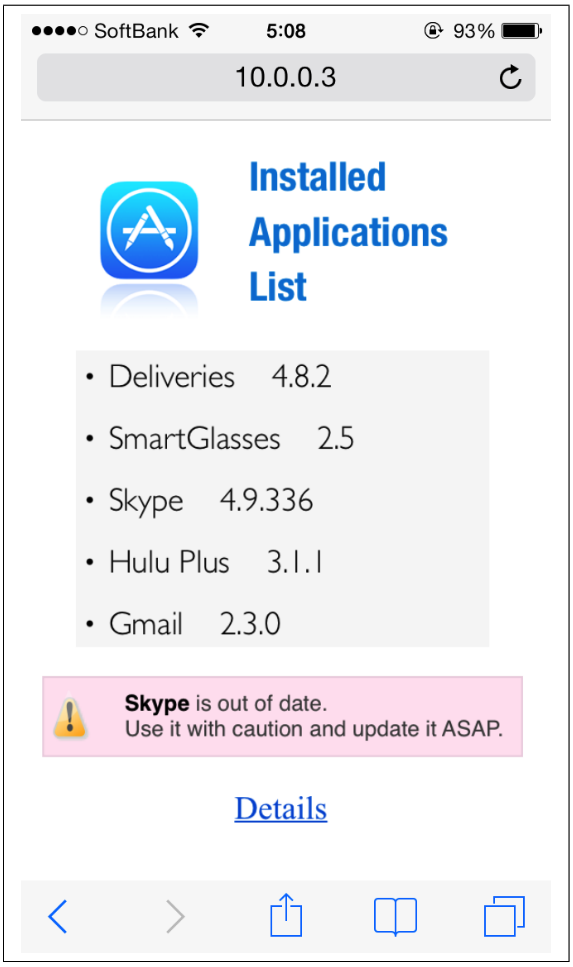
Based on your IP address:
- redacted -

You are outside of the organization, but inside of Japan

Configuration Profile Domestic will be pushed to your device.

Click to see the details of the profile

Fig 5: Web application



Installed Applications List

- Deliveries 4.8.2
- SmartGlasses 2.5
- Skype 4.9.336
- Hulu Plus 3.1.1
- Gmail 2.3.0

Skype is out of date.
Use it with caution and update it ASAP.

Details

Fig 6: Installed applications check function

by the status of the Apple's servers. However, in normal conditions, the whole process does not take more than 1 second. This is quite satisfactory. Because as far as we know, this result is not just faster than the conventional MDM system with administrator change the settings manually, but also faster than just updating a configuration profile in the user's device with Apple's genuine MDM service [14]. Of course, the vulnerabilities check function is still in development, the result will be updated in the future.

We also plan to set up a number of different episodes with different risks, and let the users actually test the system in each episode to see whether it works properly. In this test, we do not only pay attention to the correctness or the response time, but also want to know the usability of our proposed system, especially for those users without much knowledge about mobile devices. This test will be completed in the next few months.

6 Future work and Conclution

In this paper, we propose a new MDM system combined with risk analysis module to deal with the shortcomings of the conventional MDM systems. We also developed a prototype system, which supports Apple's iOS devices to verify our theory. Due to our test result, we believe that the proposed system is very practical for a large organization to manage their employees' iOS devices. It can handle the environmental risks in real time and operate without either user or administrator's interaction.

Next step, we will improve the system, make it more intelligent and powerful. The configuration profiles should be created dynamically instead of the statical way in our prototype system. We will also import more databases to the risk analysis module to optimize the vulnerabilities check function. And if possible, we will deploy this system to Android to see whether everything still goes well.

References

[1] Adrian Leung, *A mobile device management framework for secure service delivery*, Information Security Technical Report, pp. 118-126, August 2008

[2] Keunwoo Rhee, Woongryul Jeon, Dongho Won, *Security Requirements of a Mobile Device Management System*, International Journal of Security and Its Applications Vol. 6, No. 2, pp. 353-358, April 2012

[3] Sandeep Adwankar, Sangita Mohan, Vasudevan, V, *Universal Manager: seamless management of enterprise mobile and non-mobile devices*, 2004 IEEE International Conference, pp. 320-331, 2004

[4] Liu, L, Moulic, R., Shea, D, *Cloud Service Portal for Mobile Device Management*, 2010 IEEE 7th International Conference, pp. 474-478, 2010

[5] Keunwoo Rhee, Sun-Ki Eun, Mi-Ri Joo, Jihoon Jeong, Dongho Won, *High-Level Design for a Secure Mobile Device Management System*, Human Aspects of Information Security, Privacy, and Trust Lecture Notes in Computer Science Volume 8030, pp. 348-356, 2013

[6] Wonjoo Park, Sun Joong Kim, Kee Seong Cho, *Framework for security management of mobile devices*, 9th Communications and Information Technology, 2009

[7] Hyeokchan Kwon, Sin-Hyo Kim, *Efficient Mobile Device Management Scheme Using Security Events from Wireless Intrusion Prevention System*, Ubiquitous Information Technologies and Applications Lecture Notes in Electrical Engineering Volume 214, pp. 815-822, 2013

[8] Kristen Dietiker, *Managing iOS mobile devices*, 39th ACM annual conference on SIGUCCS (SIGUCCS '11), pp. 49-52, 2011

[9] National Vulnerability Database, National Institute of Standards and Technology, 2012
`http://nvd.nist.gov/`

[10] Configuration Profile Reference, iOS Developer Resources, Apple Inc, 2013
`https://developer.apple.com/library/prerelease/ios/navigation/`

[11] David Schuetz, *Inside Apple's MDM Blackbox*, Blackhat USA 2011
`https://www.blackhat.com/html/bh-us-11/bh-us-11-archives.html/`

[12] Mell P, et al, *The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems*, NIST Interagency Report 7435, 2007

[13] Japan Vulnerability Notes, JPCERT/CC and IPA, 2012
`http://jvn.jp/`

[14] Profile Manager, OS X Server
`http://www.apple.com/osx/server/`