SCIS 2016 2016 Symposium on Cryptography and Information Security
Kumamoto, Japan, Jan. 19-22, 2016
The Institute of Electronics, Information and Communication Engineers

Securing BYOD with Mobile Device Management based on SCAP and SE Android

Chung-Huang Yang (楊中皇)* Lun-Ming Tung (董倫銘)

Abstract: As popularity of the mobile devices, including smartphones and tablets, continues to grow, more and more personal data inevitably stored inside these devices and it has become an important issue to protect private data on the devices. Many organizations have adopted Bring Your Own Devices (BYOD), allowing employees to use their personal mobile devices at work. But, both personal-owned and corporate-owned mobile devices came with security risks.

Since the protection of private data on mobile devices could not be achieved with a single measurement, we designed and implemented centralized management system for Android devices based on SCAP (Security Content Automation Protocol) and SE Android. Automated configuration management based on SCAP will reduce time effort for user to setup one's mobile device with recommended configuration, while SE Android allow dynamically manage of security policy such as permission management.

Keywords: BYOD, SCAP, Configuration Management, AOSP, Permission Management

1 Introduction

Worldwide shipments of smartphones exceeded 1.2 billion units in 2014 [8]. Mobile devices, including smartphones and tables, have oversold desktop and laptop computers in recent years. Personal private data inevitably stored inside these mobile devices, and it has become an important issue to protect private data on the devices.

More and more organizations have adopted Bring Your Own Devices (BYOD) [2,9], allowing employees to use their personal mobile devices at work. Both personal-owned and corporate-owned mobile devices came with security risks. Each stolen or lost phone opens the organization up to the chance of a breach of corporate data. Organizations also might be vulnerable due to poorly configured mobile devices that are connected onto corporate networks.

Mobile device are an easy target for the attackers. Edward Snowden, former employer of the US National Security Agency (NSA), revealed that both the NSA and UK's GCHQ developed capabilities to take advantage of "leaky" smartphone apps [3]. Researchers have proposed various approaches to safeguard the mobile devices [5-7,14], but at present there is no way to guarantee the security of mobile devices and smartphones become next frontier in cybersecurity [15].

Security Content Automation Protocol (SCAP) [11] was introduced by NIST (National Institute of Standards and Technology) in 2006 and SCAP can be used for management of configuration settings. Starting with Android 4.3, Security Enhancements for Android (SE Android) [4,12] had been included to enforce mandatory access control (MAC).

In this research, we designed and implemented a centralized mobile device management (MDM) [13] system to automatically evaluate configuration setting of Android devices and to provide permission management of Android devices. Our implementations have been tested on Google Nexus 6P smartphone and Nexus 9 tablet.

*高雄師範大學 National Kaohsiung Normal University, 116, Ho Ping First Road, Kaohsiung 802, Taiwan. Email: chyang@nknu.edu.tw

2 Mobile Device Management (MDM)

Mobile device management (MDM) [2,13] is a methodology to control mobile devices. Features of MDM might include app management, network management, security management, etc. MDM approaches usually consist of a centralized server and an agent installed in the users' mobile device. Typical client/server approach would closely resemble the behavior of open source AndroRAT (Android Remote Administration Tool), https://github.com/DesignativeDave/androrat. Fig. 1 shows the basic idea of the developed MDM system. MDM agent is distributed and installed on the Android device and receive instructions from the MDM server.

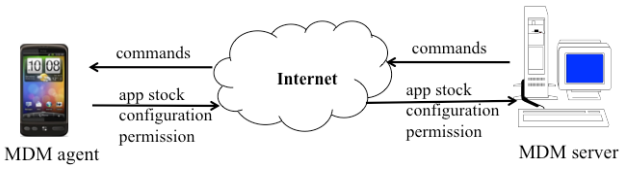

Figure 1: Mobile device management (MDM) system

In this research, our MDM server are running Ubuntu and we adopt the Android Open Source Project (AOSP) [1,16] approach to implement MDM agent for manage permission of Android devices. AOSP's SEAndroidManager and SEAndroidAdmin on AOSP offer setting and policy management of Android devices.

3 Configuration Management for Android Devices

The Security Content Automation Protocol (SCAP) [11] is a suite of specifications that standardize the format and nomenclature by which security software products communicate software flaw and security configuration information. Improper configuration setting (e.g., too small passcode length) of mobile devices might cause security risks. We use SCAP to provide a standardized approach for configuration management of mobile devices.

In the previous research [10,17], we gave preliminary implementation results of SCAP-based configuration management for iOS devices and Android devices. Fig. 2 illustrates system architecture of the developed configuration management of Android devices based on SCAP.

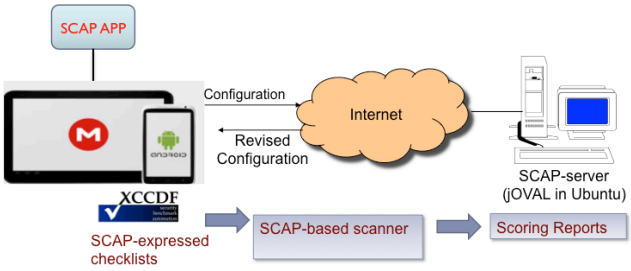

Figure 2: Architecture for configuration management of Android devices

A proprietary app was designed and implemented to read and write configuration setting of Android devices. Then configuration file will submit to the jOVAL-based SCAP server for scoring report against recommended configuration. User could revise configuration manually for further evaluation or user could download recommended configuration file and transfer the file to Android device with the proprietary app.

4 Permission Management for Android Devices

Security-enhanced Linux (SELinux) [4,12] is an open-source project that provides a mechanism for supporting mandatory access control (MAC) to various Linux distributions. Security Enhancements for Android (SE Android) was included in the Android 4.3 with permissive mode and Android moves to full enforcement since the Android 5.0 release.

Android forces apps to declare the permissions they require when use install them. There are different categories of permissions each Android app has, for example, camera, contacts, location, microphone,…, etc.

The AOSP source codes include SEAndroidAdmin for controlling settings and policy. We created an MDM agent app with source code from SEAndroidAdmin so the MDM server could decide what permission is allowed on Android device.

Although Android 6.0 Marshmallow came with partial permission management that user could manage a single app's permissions. The proposed

permission management allow MDM server send commands to MDM agent to turn-on or turn-off permission across all apps, shown in Fig. 3.

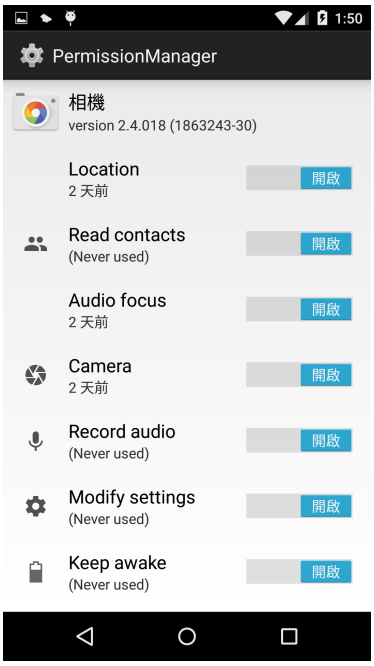

Figure 3: Permission management of Android devices

5 Conclusions

In this research, we developed a centralized mobile device management (MDM) system for Android devices based on SCAP and SE Android. Such MDM system could automatically manage configuration setting and permissions on Android devices. We are currently in the process of adding additional security features on the MDM system. Also, at present, we have two separate software on the Android device, one for configuration management and the other for permission management. Therefore, we would like to combine them into a single app.

6 Acknowledgement

This work was supported in part by research grants (102-2221-E-017-003-MY3) from the Ministry of Science and Technology of Taiwan.

References

[1] Android Open Source Project (AOSP), https://source.android.com

[2] A. Armando, G. Costa, L. Verderame, and A. Merlo, "Securing the "Bring Your Own Device" Paradigm," *Computer*, Vol. 47, No. 6, pp. 48-56, June 2014.

[3] J. Ball, "Angry Birds and 'leaky' phone apps targeted by NSA and GCHQ for user data," *The Guardian*, January 28, 2014.

[4] W. Confer and W. Roberts, *Exploring SE for Android*, Packt Publishing, 2015.

[5] J.J. Drake, Z. Lanier, C. Mulliner, P.O. Fora, S.A. Ridley, and G. Wicherski, *Android Hacker's Handbook*, John Wiley & Sons, Inc., 2014.

[6] Nikolay Elenkov, *Android Security Internals*, No Starch Press, 2014.

[7] P. Faruki, A. Bharmal, V. Laxmi, V. Ganmoor, M.S. Gaur, M. Conti, and M. Rajarajan, "Android Security: A Survey of Issues, Malware Penetration, and Defenses," *IEEE Communications Surveys & Tutorials*, Vol. 17, No. 2, 2015, pp. 998-1022.

[8] Gartner, Inc., "Smartphone Sales Surpassed One Billion Units in 2014," March 3, 2015. http://www.gartner.com/newsroom/id/2996817

[9] J. Keyes, *Bring Your Own Devices (BYOD) Survival Guide*, CRC Press, 2013.

[10] C.L. Kuo and C.H. Yang, "Security Design for Configuration Management of Android Devices," *Proc. 2015 IEEE 39th Annual International Computers, Software & Applications Conference (COMPSAC 205)*, pp. 249-254, Taichung, Taiwan, July 2015.

[11] NIST, Security Content Automation Protocol (SCAP), http://scap.nist.gov/

[12] S. Smalley, "SELinux in Android Lollipop and Marshmallow," *Linux Security Summit 2015*, Aug 2015.

[13] M. Souppaya and K. Scarfone, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, NIST Special Publication 800-124, Rev. 1, June 2013.

[14] J. Tyler, *XDA Developers' Android Hacker's Toolkit*, John Wiley & Sons, 2012.

[15] D. Yadron, "Smartphones Become Next Frontier in Cybersecurity," *The Wall Street Journal*, July 31, 2014.

[16] K. Yaghmour, *Embedded Android*, O'Reilly Media, Inc., 2013.

[17] C.H. Yang and C.M. Chen, "Configuration Management of iOS Devices based on SCAP," *Proc. The 31th Symposium on Cryptography and Information Security*, Kagoshima, Japan, Jan. 2014.