Accepted Manuscript

A root privilege management scheme with revocable authorization for Android devices

Yu-an Tan, Yuan Xue, Chen Liang, Jun Zheng, Quanxin Zhang, Jiamin Zheng, Yuanzhang Li

PII: S1084-8045(18)30025-0

DOI: 10.1016/j.jnca.2018.01.011

Reference: YJNCA 2053

To appear in: *Journal of Network and Computer Applications*

Received Date: 11 May 2017

Revised Date: 18 January 2018

Accepted Date: 20 January 2018

Please cite this article as: Tan, Y.-a., Xue, Y., Liang, C., Zheng, J., Zhang, Q., Zheng, J., Li, Y., A root privilege management scheme with revocable authorization for Android devices, *Journal of Network and Computer Applications* (2018), doi: 10.1016/j.jnca.2018.01.011.

A root privilege management scheme with revocable authorization for Android devices

Yu-an Tan[a], Yuan Xue[a], Chen Liang[a], Jun Zheng[a], Quanxin Zhang[a], Jiamin Zheng[a], Yuanzhang Li*[a,b]

[a] *School of Computer Science and Technology, Beijing Institute of Technology, Beijing 100081, China*
[b] *Research Center of Massive Language Information Processing and Cloud Computing Application, Beijing 100081, China*

Abstract

As a critical part in mobile cloud computing, the vulnerability of Android devices can directly affect the security of the mobile cloud. The unsecured Android can be potentially exploited by malwares to obtain the root privilege. Root privilege misuse is the critical issue for Android security, which breaks the integrity of Android security and rises the risk of permission escalation from malwares. The existing solutions still fail to balance the trade-off between the users desires on using root privilege and the Android security, which lays risks in leading to the root privilege misuse. To address this issue, a root privilege management scheme named Root Privilege Manager (RPM) is proposed, which adopts the root privilege access control to guarantee the exclusive root access opportunity of the authenticated apps. RPM verifies the authorization and integrity of root requesting apps based on the extracted authorization files during app installation, and then root access management controls the granting of root privilege based on the authenticated results. In this way, the end users are free from the embarrassment of appropriate decision-making while confront root access management. The prototype of RPM is implemented to evaluate its effectiveness, efficiency and performance. The experiments show RPM can effectively control the granting of root privilege and the time consumption in root access management is increased by 0.21%-0.94% respectively compared with the user management.

Keywords: Mobile cloud computing; Android security; root privilege management; revocable authorization;

1. Introduction

Security risk in mobile cloud services has been regarded as an essential issue for the researchers and the service providers of cloud computing[1, 2, 3, 4, 5, 6]. As a critical party in Mobile cloud computing, the vulnerability of mobile devices (software and hardware security issues) can directly affect the security of the mobile cloud[7, 8, 9, 10, 11]. For instance, Android devices are compromised by viruses, Trojan horses, adwares, backdoors, spywares and so on and controlled to attack the mobile cloud service[12, 13, 14, 15, 16, 17, 18]. According to a recent report[19], Twitoor, the first known botnet malware in Android, can recruit devices into an Android botnet in an unpredictable way and receive instructions for actions such as downloading secondary payloads and switching to another account to control infected devices[20, 21].

To mitigate the security threats[18, 22, 23, 24, 25], the root privilege, the crucial role in the Android security model, is strictly controlled and accessed only by some specific system services[26, 27, 28, 29]. However, the restriction can be broken through by end users via rooting tools, which provides the full control of root privilege to end users[30, 31]. Rooted Android devices bring end users conveniences such as modifying system parameters, uninstalling pre-installation apps, monitoring app behaviors and installing the third-party Android OS[26, 31]. Unfortunately, the misuse of root privilege may seriously impact the entire system security[16]. For instance, under the user management, the root privilege is arbitrarily assigned to an app which has not been verified. This is leaded by the inexperienced management by end users, which provides the root access to malwares. Once the malwares obtain the root privilege, the entire Android system security and user private data will be threats of malicious chargeback, privacy theft and system damages[30].

Considering the harmfulness of misuse[16, 32, 33], the protection and prevention schemes of root privilege are intensively studied in industry and academia [34, 35, 36, 37]. In academic, the Android system hardening approaches from different perspectives are proposed to prevent the root privilege leakage, which contains a hardening kernel and Mandatory Access Control (MAC). The kernel hardening techniques reduce the risk of root privilege leakage, which makes kernel vulnerabilities difficult to be exploited. Knox proposed by Samsung is a security solution based on the open source platform of Android, which protects the kernel integrity through its real-time kernel protection scheme, such as preventing the malicious modifications or injections to kernel. The MAC is employed to mitigate the threats from the exploitation of any daemon with root privilege, which effectively restricts the call of the critical resource, such as the SEAndroid[35], the FlaskDroid[27], and the EASEAndroid[38].

In industry, the SEAndroid[35] is practically introduced and deployed in Android 4.4 and later versions to enforce the security of the entire system. Predictably, the existing faults have been improved, including the abuse of root privileges and critical steps of exploitation. Furthermore, Knox[36, 37], the security enhancement scheme through the combination of software and hardware, is implemented in Android devices produced by Samsung, and used to enhance the access control security of