Poster: Sdguard — An Android Application Implementing Privacy Protection and Ransomware Detection

Shuangxi Hong Chuanchang Liu Bingfei Ren Junliang Chen
hongshuangxi_2008@126.com{lcc3265, rbf, chjl}@bupt.edu.cn
State Key Laboratory of Networking and Switching Technology of
Beijing University of Posts and Telecommunications
Beijing, 100876, China

Keywords

Android System; FUSE Filesystem; Permission Control; Ransomware

Currently, the smartphone has become an essential communication and amusement tool, which has strong computing power and a variety of functions. Especially, the market share of smartphone with android system account for 84% in 2016[1]. Under android system, a large of privacy data (e.g. photos or videos) are stored in external storage (emulated Sdcard storage), which can be accessed by installed apps. This not only results in privacy leakage but also incurs ransomware attack[2] (e.g. simplocker). Therefore, we present Sdguard, an app, can implement fine-grain permission control based on Linux DAC mechanism， and detect ransomware which encrypts content of file stored in external storage or lock user screen.

To install Sdguard app, we need to ensure that the smartphone has been rooted and use FUSE filesystem on external storage. During installing, sdcard daemon of android (i.e. FUSE daemon) is replaced by our customized sdcard daemon. After rebooting system, the customized daemon is loaded, and each component of Sdguard is running.

Figure 1 shows the architecture of the Sdguard app, which consists of two service components (activity stack monitor and I/O log analyzer) and an access control list. When an app creates a file, the customized FUSE daemon modifies owner and group of the file according to UID and GID of the app. Meanwhile, when an app read or write a file, the module of permission checker verifies its UID and permission to determine access action (allowing or refusing). I/O recorder can record all I/O operations to external storage, and then write log to a file. I/O log analyzer parses log file to try finding malicious action. We also create some decoy files which can be accessed by installed apps. We can find one type of ransomware which encrypts file. User can set some specific access rules to installed apps through access control list. This can meet some personal demand of user. The activity stack monitor service is in charge of monitoring activity stack of android system. The monitor only observes an activity which locates top stack. When finding an activity of certain app except lock-screen app (android system app) locates top stack for long time, we may think the app is ransomware which can lock user screen and kill its process to eliminate threat.

To enable monitoring activity stack, and starting automatically, the Sdguard application must delear related permissions, such as GET_TASK and RECEIVE_BOOT_COMPLETED. In short, the Sdguard app may be easily installed by manual way or OTA on the most of android version, and prevent privacy leakage from external storage. A user can grant/revoke certain permissions to an installed application through modifying Access control list. In addition, the Sdguard also effectively eliminate influence of ransomware.

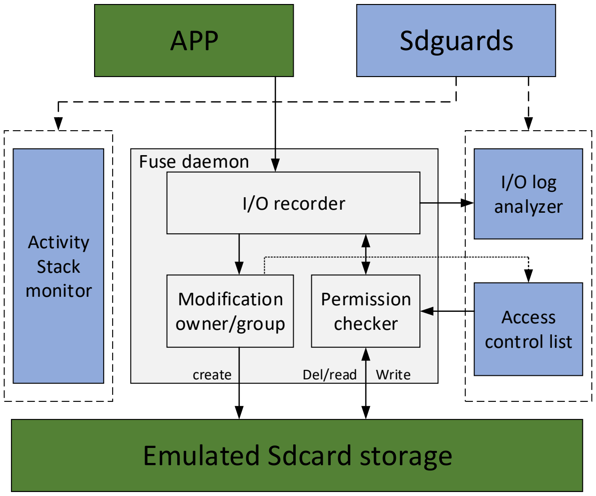

Figure 1: Sdguard app architecture and its component

This work has been sponsored by National Natural Science Foundation of China under (Grant No. U1536112), National Grand Fundamental Research 973 Program of China under (Grant No. 2013CB329102). The authors would also like to thank reviewers for their constructive comments.

REFERENCES

[1] 2016. android OS of global smartphone shipments.[Online]. Available: https://www.statista.com/statistics/236027/globalsmartphone-os-market-share-of-android/

[2] ANDRONIO, N., ZANERO, S., and MAGGI, F., 2015. HelDroid: Dissecting and Detecting Mobile Ransomware. In *Research in Attacks, Intrusions, and Defenses: 18th International Symposium, RAID 2015, Kyoto, Japan,November 2-4, 2015. Proceedings*, H. BOS, F. MONROSE and G. BLANC Eds. Springer International Publishing, Cham, 382-404. DOI= http://dx.doi.org/10.1007/978-3-319-26362-5_18.

MobiSys'17, June 19-23, 2017, Niagara Falls, NY, USA
© 2017 Copyright is held by the owner/author(s)
ACM ISBN 978-1-4503-4928-4/17/06.
http://dx.doi.org/10.1145/3081333.3089293