Poster: TrustGyges: A Hidden Volume Solution with Cloud Safe Storage and TEE

Wendi Feng, Chuanchang Liu, Bingfei Ren, Bo Cheng, Junliang Chen
State Key Laboratory of Networking and Switching Technology
Beijing University of Posts and Telecommunications, 100876, PRC
{logan,lcc3265,rbf,chengbo,chjl}@bupt.edu.cn

CCS CONCEPTS

• **Information systems** → *Storage management*; • **Security and privacy** → *Access control*;

1 INTRODUCTION

As smartphones are becoming ubiquitous, mobile security has been a big concern to users. Especially when users employ their phone both for work and personal use, which is prone to lead to compromising their working secret. Because attackers may compulsorily or secretly install monitoring or detective programs on the regular smartphone system like Android[1]. Simply storing sensitive data on the phone or simply separating the sensitive storage from normal files without managing the storage procedure make the sensitive data vulnerable. For example, undercover reporters trying to reveal illegal activities with the smartphone, they have to prevent the suspects from discovering the evidence data and running differences (especially IO operations) of the smartphone system to protect their personal safety. Former hidden volume solution failed to address runtime attacks, which makes the phone vulnerable. In this paper, we present TrustGyges, a hidden volume based data hiding mechanism, with the idea of TrustShadow [1], by adopting Trusted Execution Environment (TEE) technology to avoid threats especially at disk mounting time on the Android. With that, users can protect their sensitive data with confidentiality and integrity.

2 TRUSTGYGES MECHANISM

TrustGyges consists of HiddenVolume, TEE and CloudSafeStore. Sensitive data is stored on the HiddenVolume locally on the phone. HiddenVolume creation is represented as a triad $\langle Dev_f, Tab, Dev_t \rangle$. Firstly, blocks are selected randomly from the `userdata` partition Dev_f. Then, the HiddenVolume Dev_t is created by exploiting device mapper technology with the mapping table Tab. Tab contains information of mapping partition blocks, mapping rules and the mapped device blocks. Next, the HiddenVolume is formatted with a file system. Finally, the HiddenVolume is mounted for use. Storing Tab solely locally is prone to compromise. Because malwares may steal or destroy Tab. Therefore, an account will be created on the Cloud safe storage for each user to save the Tab. Besides, to avoid being discovered by adversaries while getting Tab, TrustGyges adopts TEE (e.g. ARM TrustZone[2]) to retrieve the Tab from the CloudSafeStore safely. So, Each time, user wants to use the HiddenVolume, TrustGyges will fetch Tab from the server. And HiddenVolume will be mounted for storing sensitive data. TrustGyges uses Google's gRPC tool to fetch the Tab metadata stored on the cloud. The exchanging data format is Protocol Buffer, which is smaller, faster and simpler and suitable for mobile platforms. Besides, to avoid man in the middle attack, gRPC uses TLS to encrypt all the data transferred between CloudSafeStore and the device. Figure 1 depicts the whole process of getting the storage block metadata. HiddenVolume design and implementation can be found in our previous work [2]. Since the phone may not always connect to the Internet while using the HiddenVolume, the system may insufficient to get the location information instantly. So a cached version from RPMB partition will be used for availability.

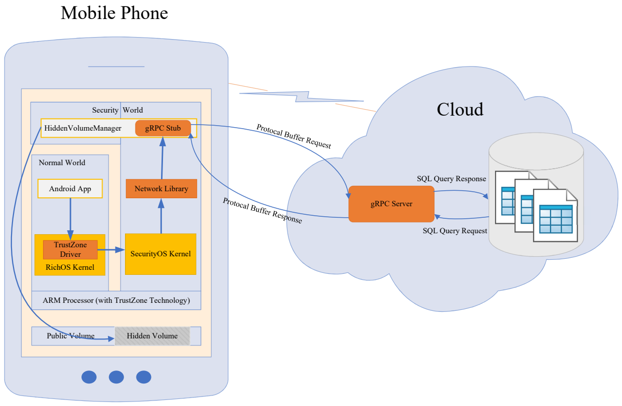

Figure 1: Structure of TrustGyges. Normal OS App have TEE sends requests and manage the hidden volume.

ACKNOWLEDGMENTS

The work is supported by the National Natural Science Foundation of China (Grant No.U1536112).

REFERENCES

[1] Guan, L., and et. al. Trustshadow: Secure execution of unmodified applications with arm trustzone. In *Proceedings of the 15th Annual International Conference on Mobile Systems, Applications, and Services* (New York, NY, USA, 2017), MobiSys '17, ACM, pp. 488–501.

[2] Hong, S., Liu, C., Ren, B., Huang, Y., and Chen, J. Personal privacy protection framework based on hidden technology for smartphones. *IEEE Access* (2017).

[1] https://www.android.com/

[2] https://www.arm.com/products/security-on-arm/trustzone

MobiSys '18, June 10–15, 2018, Munich, Germany
© 2018 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-5720-3/18/06.
https://doi.org/10.1145/3210240.3210803