# Memory Data Protection on TrustZone Enabled Platform (Poster Abstract)

Xianyi Zheng[1,2] Gang Shi[1,2] Dan Meng[1,2]

[1] Institute of Information Engineering, Chinese Academy of Sciences, Beijing, China
[2] University of Chinese Academy of Sciences, Beijing, China
{zhengxianyi, shigang, mengdan}@iie.ac.cn

**Abstract.** Although there are great advances in systems security, the malicious attacks accessing the critical data in the Rich OS (ROS) still pose a real threat [1]. Furthermore, the monolithic ROSes, such as Windows, Mac OS X, Linux, and FreeBSD, lack sufficient protection mechanisms to protect these critical data. As a result, ROSes define and store access control policies in main memory which any code executing within the kernel can modify [2]. Therefore, we propose a memory data protection mechanism on smartphones enabling TrustZone technology. The address space of the whole process is divided into two domains: the plain domain and the cipher domain. The plain domain stores these frequently used memory pages recently and the cipher domain encrypts these less used memory pages. Specifically, we firstly acquire the ratio between the frequently using memory pages and less using memory pages by analyzing the usage rate of the processes using memory pages, then we divide the memory pages into the plain domain and the cipher area domain according to the division rate. These memory pages which are not used recently will be moved to the cipher domain according to the Least Recently Used (LRU) algorithm and these memory pages which are most likely to use will be decrypted from the cipher domain and moved to the plain domain according to the prefetching mechanism when the system is running. The cipher domain deploying in the secure world protected by TrustZone technology provides the crypto services, such as RSA, DES, AES and et al, and the crypto key is stored in the secure world permanently which is impossible to be acquired by attackers from the ROS. However, according to the local principle of code usage, the performance consumption brought by these memory data moving into or out the cipher domain in the secure world should be in the acceptable range. Thus, we can ensure that the most of memory data will not be compromised and stolen by malicious attackers because the cipher domain is protected in the secure world even if the ROS compromised or even crashed.

**Keywords:** the cipher domain, the plain domain, ARM TrustZone

## Reference

1. Ahmed M A., Peng Ning., et al. Hypervision across worlds: real-time kernel protection from the ARM TrustZone secure world. In: CCS 2014. pp. 90-102 (2014)
2. Nathan, N., Theodoros, K., et al. Nested Kernel: An Operating System Architecture for Intra-Kernel Privildge Separating. In: ASPLOS'15. pp.191-206 (2015)