Utilizing GPU Virtualization to Protect the Private Keys of GPU Cryptographic Computation

Ziyang Wang[1,2,3], Fangyu Zheng[1,2(✉)], Jingqiang Lin[1,2,3], and Jiankuo Dong[1,2,3]

[1] Data Assurance and Communication Security Research Center, CAS, Beijing 100093, China
{wangziyang,zhengfangyu,linjingqiang,dongjiankuo}@iie.ac.cn
[2] State Key Laboratory of Information Security, Institute of Information Engineering, CAS, Beijing 100093, China
[3] School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China

Abstract. Nowadays graphics processing units (GPUs) have become popular parallel computing platforms known as General-Purpose GPU (GPGPU) computing. GPUs thereby are chosen by some security researchers as cryptographic accelerators to secure massive volumes of transactions. However, their security issues are ignored in spite of their popularity and performance. There are some possible information leakages faced with malicious attacks or even in the normal GPU computing. Our objective is to secure the confidentiality of cryptographic keys in GPU computing environments and provide easy-to-use programming with few constraints. In this paper, we propose a prototype in Linux, a system of GPGPU computing solution empowered by GPU virtualization technology, which keeps encrypted keys in guest machine to protect secret keys from leakage even in the event of full system compromise. With the API interception and redirection of CUDA, applications in Virtual Machines (VMs) can access the GPU device in a transparent way. Besides, we use `virtio`, a dedicated virtual I/O device, to transfer data between virtual and host machines in high performance. In our current study, we evaluate our prototype with the GPU implementation of ECC. We show that it can protect private keys of GPU cryptographic computation and it also incurs low performance penalty compared with the native environment, therefore demonstrating the prototype is secure and requires reasonable overhead.

Keywords: GPU · GPGPU · GPU virtualization
Information leakage · Isolation

This work was supported by National Natural Science Foundation of China under Award no. 61772518.

D. Naccache et al. (Eds.): ICICS 2018, LNCS 11149, pp. 142–157, 2018.
https://doi.org/10.1007/978-3-030-01950-1_9