Security Overview on Secure Encrypted Virtualization

Robert Buhren
Technische Universität Berlin

30th Crypto Day, 28/29 March 2019

Cloud computing has become indispensable in today's computer landscape. The flexibility it offers for customers as well as for providers has become a crucial factor for large parts of the computer industry. Virtualization is the key technology that allows for sharing of hardware resources among different customers. The controlling software component, called hypervisor, provides a virtualized view of the computer resources and ensures separation of different guest virtual machines.

However, this important cornerstone of cloud computing is not necessarily trustworthy or bug-free. To mitigate this threat, AMD introduced Secure Encrypted Virtualization, short SEV, which transparently encrypts a virtual machines memory (Kaplan, Powell & Woller (2016)).

Due to the fact that the hypervisor is still tasked with the resource management of the guest system, a malicious cloud-provider can still access confidential guest memory as previous research has shown (Morbitzer, Huber, Horsch & Wessel (2018); Hetzelt & Buhren (2017)).

In this talk I will present the current state of research revolving the SEV technology and give an overview on the previously presented attacks.

References

Felicitas Hetzelt & Robert Buhren (2017). Security analysis of encrypted virtual machines. In *ACM SIGPLAN Notices*, volume 52, 129–142. ACM.

David Kaplan, Jeremy Powell & Tom Woller (2016). White Paper AMD Memory Encryption. `http://amd-dev.wpengine.netdna-cdn.com/wordpress/media/2013/12/AMD_Memory_Encryption_Whitepaper_v7-Public.pdf`.

Mathias Morbitzer, Manuel Huber, Julian Horsch & Sascha Wessel (2018). SEVered: Subverting AMD's Virtual Machine Encryption. In *Proceedings of the 11th European Workshop on Systems Security*, 1. ACM.

crypto day matters 30 (2019)
Beiträge vom 30. Kryptotag, 28.-29.03.2019, Mozilla, Berlin.
doi:10.18420/cdm-2019-30-26