Insecure Until Proven Updated: Analyzing AMD SEV's Remote Attestation

Robert Buhren
Technische Universität Berlin

31st Crypto Day, 17/18 October 2019

Cloud computing is one of the most prominent technologies to host Internet services that unfortunately leads to an increased risk of data theft. Customers of cloud services have to trust the cloud providers, as they control the building blocks that form the cloud. This includes the hypervisor enabling the sharing of a single hardware platform among multiple tenants. Executing in a higher-privileged CPU mode, the hypervisor has direct access to the memory of virtual machines. While data at rest can be protected using well-known disk encryption methods, data residing in main memory is still threatened by a potentially malicious cloud provider.

AMD Secure Encrypted Virtualization (SEV) claims a new level of protection in such cloud scenarios. AMD SEV encrypts the main memory of virtual machines with VM-specific keys, thereby denying the higher-privileged hypervisor access to a guest's memory. To enable the cloud customer to verify the correct deployment of his virtual machine, SEV additionally introduces a remote attestation protocol. This protocol is a crucial component of the SEV technology that can prove that SEV protection is in place and that the virtual machine was not subject to manipulation.

This talk presents the result of our security analysis of AMD's remote attestation protocol which will be presented at this year's conference on Computer and Communication Security (CCS) (Buhren, Werling & Seifert (2019)). We demonstrate that it is possible to extract *critical* CPU-specific keys that are fundamental for the security of the remote attestation protocol.

Building on the extracted keys, we propose attacks that allow a malicious cloud provider a complete circumvention of the SEV protection mechanisms. Although the underlying firmware issues were already fixed by AMD, we show that the current series of AMD Epyc CPUs, i.e., the Naples series, does not prevent the installation of previous firmware versions. We show that the severity of our proposed attacks is very high as no purely software-based mitigations are possible. This effectively renders the SEV technology on current AMD Epyc CPUs useless when confronted with an untrusted cloud provider.

To overcome these issues, we also propose robust changes to the SEV design that allow future generations of the SEV technology to mitigate the proposed attacks.

crypto day matters 31 (2019)
Beiträge vom 31. Kryptotag, 17.-18.10.2019, Qualcomm, Berlin.
doi:10.18420/cdm-2019-31-25

References

Robert Buhren, Christian Werling & Jean-Pierre Seifert (2019). Insecure Until Proven Updated: Analyzing AMD SEV's Remote Attestation URL http://arxiv.org/abs/1908.11680.