Title: A Scattering Technique for Protecting Cryptographic Keys in the Cloud

Speaker: Khaled Salah

Abstract: Cloud computing has become a widely used computing paradigm providing on-demand computing and storage capabilities based on pay-as-you-go model. Recently, many organizations, especially in the field of big data, have been adopting the cloud model to perform data analytics through leasing powerful Virtual Machines (VMs). VMs can be attractive targets to attackers as well as untrusted cloud providers who aim to get unauthorized access to the business critical-data. The obvious security solution is to perform data analytics on encrypted data through the use of cryptographic keys as that of the Advanced Encryption Standard (AES). However, it is very easy to obtain AES cryptographic keys from the VM's Random Access Memory (RAM). In this paper, we present a novel key-scattering (KS) approach to protect the cryptographic keys while encrypting/decrypting data. Our solution is highly portable and interoperable. Thus, it could be integrated within today's existing cloud architecture without the need for further modifications. The feasibility of the approach has been proven by implementing a functioning prototype. The evaluation results show that our approach is substantially more resilient to brute force attacks and key extraction tools than the standard AES algorithm, with acceptable execution time.