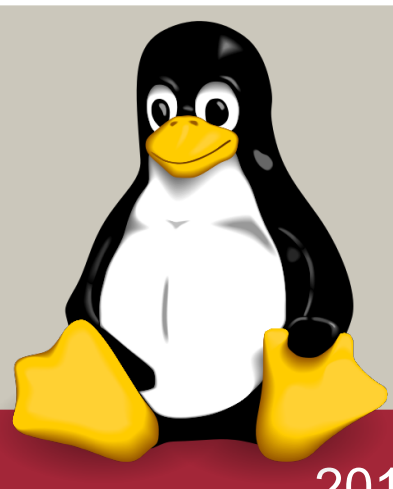
ulm university universität ulm



Bachelor Thesis

2017-07-19

Evaluating Virtual Machine Encryption

Context

Virtual Machines are present in many different areas these days: on desktop pcs, on servers or in cloud computing. Cloud computing uses virtual machines to share physical resources among multiple customers. The hypervisor, the layer which provides the encapsulation between physical server and various virtual machines, is responsible for restricting memory and disk access and guarantee the isolation between virtual machines. Yet, from a customer perspective, this hypervisor has to be trusted blindly.

While disk encryption became popular on laptops and even smartphones, the virtual machines in popular cloud computing environments are not encrypting anthing.

Scope of the Thesis

This thesis invastigates encryption of virtual machines. First, an analysis of encryption techniques and possible devices (disk, ram) will provide a conceptual overview. Second, one encryption technique will be practically evaluated on a test server with e.g. KVM as a hypervisor on a Linux operating system. The evaluation will present different use case scenarios with artificial workloads, and how these scenarios perform with and without the encryption.

Requirements and Comments

Experiences with Linux and a basic understanding of virtualization are beneficial for this bachelor thesis.

If you are interested in this or similar theses, please contact Christopher Hauser either by mail or directly in his office.

mail: christopher.hauser@uni-ulm.de
office: Uni West, 43.2.209

Faculty of Engineering and Computer Science

Institute of Information Resource Management