Technische Universität München
Chair for Network Architectures and Services
Prof. Dr. Georg Carle

BA/MA

Secure Start-Up of Virtual Machine Images

Basics

A Virtual Machine Monitor (VMM) or Hypervisor is a software component that allows that multiple virtual machines (VM) run concurrently on one physical machine. The integrity (~security) of the VMM is crucial for the integrity of the VMs. Mechanisms based on Trusted Computing (TC) technology exist that are able to start up a VMM in a specific way that guarantees the integrity of the VMM. The Trusted Platform Module (TPM), a cryptographic chip embedded on a machines mainboard, is the core component of TC and can be regarded as a hardware root-of-trust to a system.

Motivation

Our chair is researching on an architecture that is able to provide a high level of security for industrial networks. One basic idea we have is to leverage virtualization technology in order to isolate functional components of a system. E.g. monitoring/control application and the productive applications will be run in different VMs. One important task is to start up a VM in a secure way, i.e. to guarantee that the VM image has integrity. A first approach would be to use signed, disposable VM images for the productive system. Before the VM image is launched, a verification application needs to check the signature of the image. Another important aspect is how to trustworthily prove to a central monitoring server that the started VM image has integrity. For this purpose the TPM and TC mechanisms can be used.

Task Description

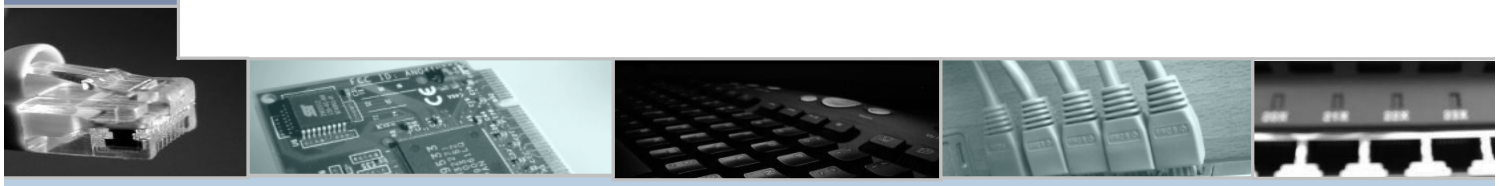
This thesis focuses on a mechanism that is able to securely start up a VM and to prove the integrity of the started VM to a central monitoring server. Your tasks are to perform a requirements analysis of the system and to design, implement and evaluate a prototype. Important parts of the evaluation are an attack analysis, a comparison of the implemented system to a solution that starts up VMs without integrity verification and a performance evaluation of the system.

Requirements

You should have interest and basic knowledge in computer/network security, virtualization technology (XEN), and operation systems. The implementation will be based upon a XEN-virtualized system and be implemented in C/C++ or Java.

Miscellaneous

Thesis can be performed in German or English. Continuation of your work as HiWi is possible.



Further Information: Holger Kinkelin / Nadine Herold [kinkelin|herold]@net.in.tum.de
Chair for Network Architectures and Services