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

BA/MA

Security and Privacy for Personalized Virtual Machine Images using Smart Cards

Basics

Smart Cards are security tokens equipped with a processor and asymmetric keys. The Smart Card provides a secure and portable environment to perform cryptographic operations. Keys are typically assigned to a specific person, hence Smart Cards are often used for digital signatures and user authentication. **Virtualization** technology provides mechanisms to host several operating systems as virtual machines (VM) on one physical machine. Virtualization is an important enabling technology for many popular services as e.g. Cloud computing.

Motivation

Virtualization is also beneficial for modern office environments or computer pools. In "virtualization-enabled" environments, users obtain a fully flexible VM instead of a login to a inflexible and restricted pre-configured operating system. VM users are able to setup, personalize and maintain the OS individually. Scenarios such as flexible workplaces become possible: whenever needed, the personalized VM image (~ the virtual machine) is pushed to a physical machine and the user is immediately able to continue his work.

Task Description

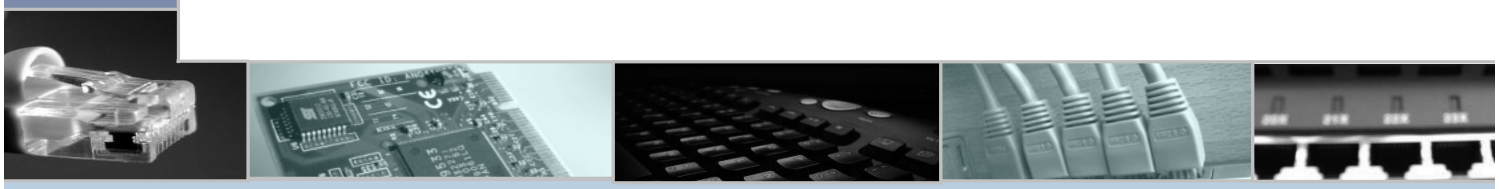
This thesis focuses on the **security and privacy of VM images**. The aim is to design, implement and evaluate a mechanism that encrypts a VM image using keying material stored on a Smart Card. The Smart Card is needed to decrypt and verify the VM image before booting the system. For a BA thesis, your tasks are to perform a thorough **analysis of requirements** of the system and the **design, implementation and evaluation** of a prototype. An important part of the evaluation will be an **attack analysis**. MA theses will be enhanced with additional questions concerning the **trustworthiness of the Hypervisor**.

Requirements

You should have interest in virtualization technology (XEN) and operating systems, as well as basic security and programming skills. Implementation is done in Java or C/C++.

Miscellaneous

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



Further Information: Holger Kinkelin kinkelin@net.in.tum.de
Chair for Network Architectures and Services