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

BA/MA

Establishing Secure Communication for (Virtual) Machines using Java Smart Cards

Basics

Java Smart Cards are small scale computing devices able to execute Java applets and to store/use cryptographic keying material. Major advantage of Smart Cards is security. E.g. malware present on a computer is not able to compromise the Smart Card, i.e to tamper the applet running on the Smart Card or to steal keys. Virtualization technology provides mechanisms to host several virtual machines (VMs) on one physical machine. Virtualization is an important enabling technology for many popular services as Cloud computing. Virtualization is also often used for secure isolation of processes/applications.

Motivation

Our chair is researching on an architecture able to provide a high level of security for industrial networks. A cornerstone of our architecture are trustworthy monitoring and control applications for machines. Currently we research on virtualization-based monitoring/control (m/c) mechanisms. Besides the security and trustworthiness of m/c applications the communication between m/c apps and a central m/c server needs to be secured. This is needed to prevent that attackers are able to fake monitoring data or to send faked control commands to machines. For securing m/c communication we plan to use an applet running on a Java Smart Card.

Task Description

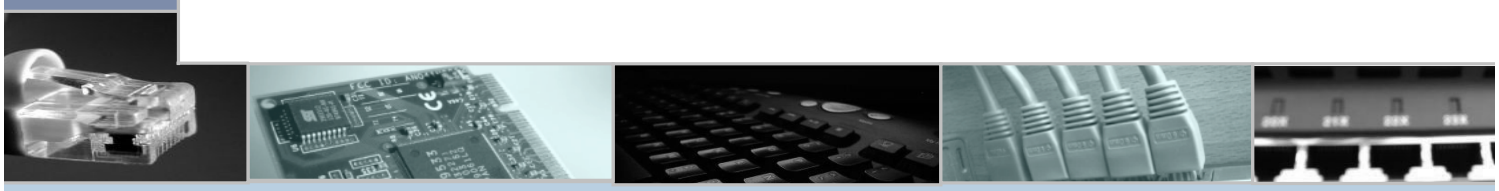
This thesis focuses on the security and privacy of m/c communication. The aim is to design, implement and evaluate a mechanism that establishes secure communication between m/c applications running within VMs and a central server using Smart Cards. The Smart Card will be used as a secure communication endpoint. 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 uses no Smart Cards and a performance evaluation of the system.

Requirements

You should have interest and basic knowledge in (network) security, Linux (network) administration, virtualization technology (XEN) and 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