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

BA / MA

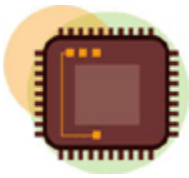
Runtime Integrity for Security Critical Processes

Basics

In the AutHoNe (Autonomic Home Networking) Project we develop security mechanisms that are intended (but are not limited) to be used within home networks. The central element of our security infrastructure is a local certification authority (Home CA) that issues certificates to user's devices.

Motivation

The protection of the Home CA's private key is crucial for home network security: if the private key is stolen by an attacker, she is able to generate authentic certificates for her devices that provide access to the home's services and data.



In previous work we leveraged the Trusted Platform Module (TPM), a cryptographic chip that is firmly integrated into a computer, to protect the Home CA's private key against theft. Unfortunately attacks are still possible, where malware *uses* the TPM-protected key or tricks the operator of the Home CA to sign a “bogus” certificate. Again the attacker obtains an authentic certificate.

Task Description

In this thesis, existing mechanisms and technologies need to be analyzed and leveraged that are able to guarantee the integrity (i.e. the absence of malware, etc) of a computing system during the execution of security critical processes. An example for such a process is the signing of certificates of the Home CA. After a threat analysis of the existing Home CA, a state of the art analysis of existing runtime protection mechanisms needs to be performed. After this theoretical part, a “hardened” Home CA needs to be defined and a prototype implemented and evaluated.

Requirements

Knowledge in network security and protocols, C/C++ programming, Linux skills and some geekiness.

Miscellaneous

This thesis can be performed in German or English.
You have the opportunity to stay at our chair after the thesis is finished as a student researcher (HiWi) to continue your work.

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