ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

MARIO STRASSER
<mast@gmx.net>

Semester Thesis: Virtual TPM

A Software-based TPM Emulator for Linux

Description

The *Trusted Computing Group* (TCG) – formerly known as *Trusted Computing Platform Alliance* (TCPA) – has produced open specifications for a security chip, the so called *Trusted Platform Module* (TPM) and related software interfaces. The TPM is designed to provide client machines with a minimal but essential hardware base for client-side security. It provides two important security functions: secure storage of signature and encryption keys and system software integrity measurement. TPM's secure storage can be used to protect an individual's RSA authentication private key or a filesystem's master key from theft or disclosure. TPM's integrity measurement can be used to detect software compromise, such as a rooted kernel, and to lock down use of protected keys and data if a compromise is found. In effect, it has been shown by IBM that many of the Microsoft NGSCB guarantees can be obtained on today's hardware and today's software and that these guarantees do not require a new CPU mode or operating system but merely depend on the availability of an independent trusted entity, a TPM for example.

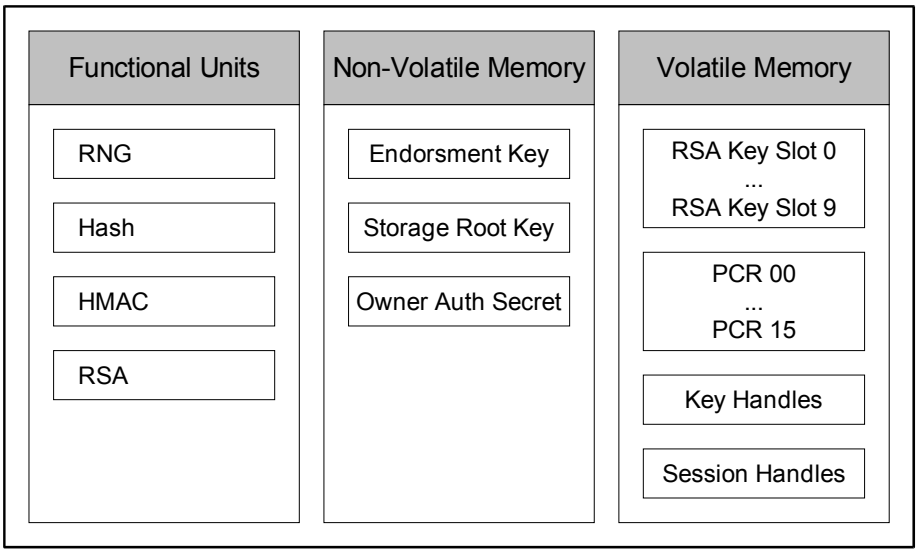

Figure 1: Trusted Platform Module (TPM)

However, although a TPM is going to be part of most state of the art personal computers in the near future, there are and will always be situations where a TPM is unavailable or unaccessible. Due to this facts and to get deeper insight into the functionality, opportunities as well as limitations or even threats of a TPM, the goal of this thesis is the implementation of a virtual (i.e., software emulated) TPM by the means of a Linux kernel module. However, as a software based module can never give one the same security guarantees as does a true hardware-based TPM, its main purposes is not its substitution but to have the ability to simulate TPMs for educational and experimental purposes.

Tasks and Goals

- Implementation of a software-emulated TPM by the means of a Linux Kernel Module. A more detailed description of which parts (i.e. commands) must/should be implemented will be prepared during the first two weeks of the thesis. The authoritative specification is the TCG TPM Specification Version 1.2.
- Implementation of the TCG Device Driver Library to access the module.
- The supported Linux kernel releases are 2.4 and 2.6.

Cooperation and Coordination

The Global Security Analysis Lab at IBM Watson Research as well as the *Enforcer*-group of the Department of Computer Science at Dartmouth College have already done a lot of research and development regarding TPM and TCG under Linux. To avoid doing redundant work and for the benefit of all, the scope of this thesis has been coordinated with their current efforts.

- David Safford <safford@watson.ibm.com>
- Omen Wild <omen.wild@dartmouth.edu>

Duration and Schedule

- Start: Monday, March 29, 2004
- Size: ~ 150 man hours
- Deadline: Friday, July 9, 2004 (not strict)
- There will be weekly meetings with the supervisors.
- A detailed project schedule and milesone plan will be prepared during the first two weeks of the thesis.

Supervision

- Paul E. Sevinç <paul.sevinc@inf.ethz.ch>
- Prof. Dr. David Basin <basin@inf.ethz.ch>

Student

- Mario Strasser <mast@gmx.net>