ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Master's Thesis for one student

Trusted KNOPPIX

Contact: paul.sevinc@inf.ethz.ch

Introduction

A Trusted Platform Module (TPM) is found in more and more computers [1, 2]. For a few years, researchers at IBM Research have been looking into how to take advantage of a TPM within a Linux-based PC [5]. Similar research has started at Dartmouth College a couple of years ago [4, 6] and resulted in an open-source project [7]: *"The Enforcer is a Linux Security Module designed to improve integrity of a computer running Linux by ensuring no tampering of the filesystem. It can interact with TCPA hardware to provide higher levels of assurance for software and sensitive data."*
Typically, Linux distributions come without TPM support, though. One such distribution is KNOPPIX [3]: *"KNOPPIX is a bootable CD with a collection of GNU/Linux software, automatic hardware detection, and support for many graphics cards, sound cards, SCSI and USB devices and other peripherals. KNOPPIX can be used as a Linux demo, educational CD, rescue system, or adapted and used as a platform for commercial software product demos. It is not necessary to install anything on a hard disk."*

Project Objective

The main objective of this project is to create a KNOPPIX distribution that includes the Dartmouth College or the IBM Research software—adapted to the latest TPMs—in order to allow for the attestation of the distribution's software stack. The software stack shall include a Java application (and thus a Java run-time environment [JRE]). If a remote server (that is in control of an enterprise) considers the software stack running on a client (that is not in control of the enterprise) to be trustworthy, it will entrust the Java application with a secret (key) that must not be disclosed to non-trusted systems. The secret may be stored on the TPM for off-line use.
The challenges of this project are:

- Adapting and extending the TPM software to the TPM specification 1.2 [8] (in C or C++)
- Modifying the KNOPPIX kernel to be TPM-aware
- Delimiting a minimal software stack that meets the stated objective and measuring it
- Designing a protocol that establishes trust towards the client at the server

- Defining guidelines for the secure handling of the secret at the client
- Implementing the server and the client (in Java)

Prerequisites

- experience in administrating (and ideally programming) Linux
- working knowledge of the Java platform (and ideally its security aspects)

Supervision

Prof. Dr. David Basin and Paul E. Sevinç (paul.sevinc@inf.ethz.ch).

References

1. heise online. *Neue Trusted Platform Modules schon im Einsatz*. <http://www.heise.de/newsticker/meldung/60040>
2. heise online. *Computex: Trusted Platform Module nach TCG-1.2 nun auch bei Infineon*. <http://www.heise.de/newsticker/meldung/60080>
3. *KNOPPIX Linux Live CD*. <http://www.knoppix.org/>
4. John Marchesini, Sean W. Smith, Omen Wild, Rich MacDonald. *Experimenting with TCPA/TCG Hardware, Or: How I Learned to Stop Worrying and Love The Bear*. <http://www.cs.dartmouth.edu/~sws/abstracts/mswm03.shtml>
5. Reiner Sailer, Leendert Van Doorn, James P. Ward. *The Role of TPM in Enterprise Security*. <https://www.trustedcomputinggroup.org/press/news_articles/rc23363.pdf>
6. Sean W. Smith. *Trusted Computing Platforms*. <http://www.springeronline.com/sgw/cda/frontpage/0,11855,4-148-22-36520721-detailsPage%253Dppmmedia%257CaboutThisBook%257CaboutThisBook,00.html>
7. SourceForge.net. *Enforcer Linux Security Module*. <http://sourceforge.net/projects/enforcer/>
8. Trusted Computing Group. TCG TPM Specification Version 1.2. <https://www.trustedcomputinggroup.org/downloads/specifications/tpm/tpm>