Seminar / Project Trusted Computing

Lightweight Trusted Platform Module in C

Abstract:

The trusted platform module (TPM) is one of the core building blocks of a trusted platform. In traditional PC-style environments, the TPM is implemented as a dedicated piece of hardware, supported by a quite large and complex trusted software stack (TSS). In embedded environments it is not desirable to have to deal with the full complexity of an independent hardware device and a full-scale trusted software stack. The primary goal of this project is to develop a lightweight software TPM on basis of the "TPM emulator" from ETH Zürich, together with a simple API for directly accessing low-level TPM commands. Finally this software TPM implementation should be embedded into a small Java VM

Start:

immediately

Participants:

1

Prerequisites:

experience in C and Java software development

IAIK TU Graz

Contact:

Johannes.Winter@iaik.tugraz.at
Kurt.Dietrich@iaik.tugraz.at