

Portable Trusted Computing using the .NET Framework

Motivation:

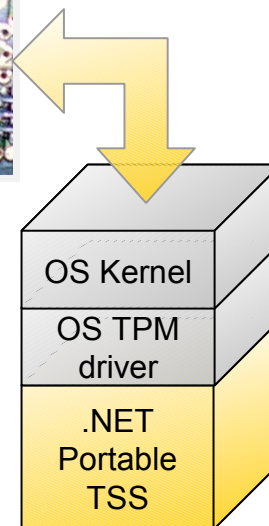
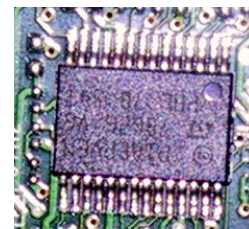
Trusted Platform Modules (TPMs) form the fundamental hardware building block for Trusted Computing on today's desktop computer platforms. These hardware building blocks are supported by a complex multi-layer Trusted Software Stack (TSS). Various commercial and open-source implementations of such software stacks exist. Two of the most popular open-source stacks are IBM's Trousers (C) and IAIK's jTSS (Java). Both of these stacks try to follow the Trusted Computing Group's TSS specifications quite closely and inherit most of the complexity of the TCG design.

Project description:

The goal of this project is to implement a portable lightweight object-oriented Trusted Software Stack for the .NET framework. Ideally this stack will be implemented purely in C# without the need for any natively compiled libraries. This project especially focuses on cross-platform interoperability. The Trusted Software Stack being implemented as part of this project should work on Microsoft's .NET runtime and on the Mono runtime without any changes.

Tasks:

- Design and implement a portable lightweight Trusted Software Stack for the .NET framework
- Design a simple to use object oriented API for the .NET Trusted Software Stack (TCG TSS compatibility is not required)



Master Project

Participants: 1-2 Students

Prerequisites:

- Experience with C# software development
- Basic understanding of cryptography and Trusted Computing

Contact:

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

Studies: INF SEW TEL Master Thesis

The master project can be continued as master thesis.