

# Practical TPM Virtualization

## Motivation

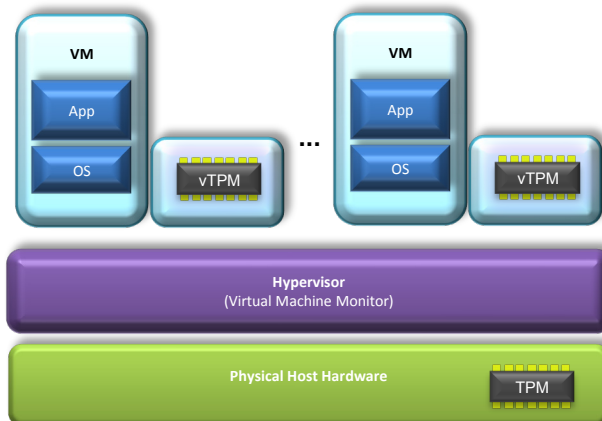
Modern computer platforms come equipped with security hardware, the Trusted Platform Module (TPM).

However, it is not designed to be shared among virtual machines.

In this project, IBM's software (v)TPM will be integrated in our acTvSM virtualization platform and a Public Key Infrastructure.

## Project description

- Practical implementation in Linux/KVM environment
- Students will gain deep understanding of Trusted Computing concepts.



## Literature

- Berger, S., Cáceres, R., Goldman, K. A., Perez, R., Sailer, R., and van Doorn, L. *vTPM: virtualizing the trusted platform module*. In Proceedings of the 15th Conference on USENIX Security Symposium - Volume 15 USENIX Association, 2006.
- acTvSM platform <http://trustedjava.sf.net>

## Deliverables

- Term paper
- Source files (in git repository)
- Documentation
- Presentation (10 .ppt slides)

## Project schedule

- Agreed between candidate and supervisor

## Curriculum

Studies:  INF  SEW  TEL  MAT  Master Thesis

Working scope and awarded credits are scalable.

## Prerequisites

- Linux
- Basic C, Basics of IT Security

## Advisor / contact

Ronald.Toegl@iaik.tugraz.at