



# Master Thesis:

## Reconstructing Lock-Keeper based on Trusted Computing

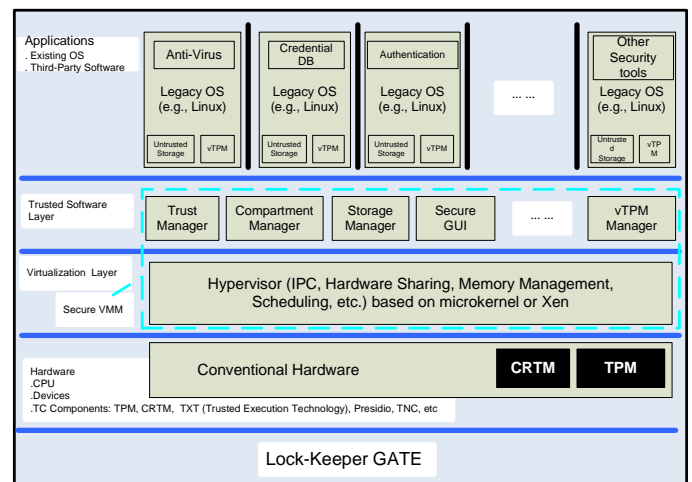
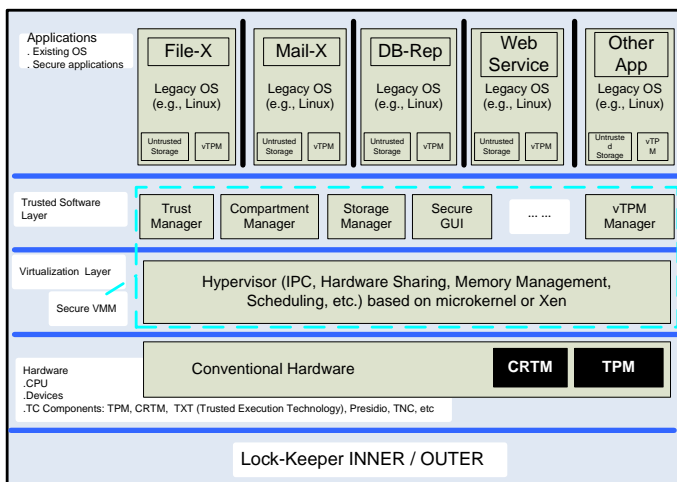
published: April 2008



As an important implementation of **Physical Separation** (PS), Lock-Keeper has been known as an efficient approach to separate private networks or sensitive hosts at any levels and permit secure data exchange simultaneously. **Trusted Computing** (TC) technology is a new solution for enhancing security of software processes and their underlying core OS. Being emerged for several years, TC has not yet been widely deployed in practice due to kinds of criticisms.

This thesis targets on applying TC concepts into Lock-Keeper to solve some security problems existing in current Lock-Keeper design. Firstly, the security of Lock-Keeper OUTER component needs to be enhanced because of the exposed connection with the external world. Secondly, there are normal operating systems and software-based application modules running on each Lock-Keeper component, which could probably be accessed, misused and even intentionally attacked. Moreover, Lock-Keeper is usually deployed on border of a network and works automatically to provide secure data exchange. A reliable way to verify working state of Lock-Keeper is required.

We expect to reconstruct the Lock-Keeper system using the TC concepts. Our requirements on (1) hardened operating system, (2) restricted system control (3) reliable remote assessment, are exactly the competences of the TC technology. On the other hand, we believe the Lock-Keeper is a perfect use case of the TC.



### Contact

Feng Cheng  
(0331) 5509-521  
feng.cheng@hpi.uni-potsdam.de

Prof. Dr. Christoph Meinel  
(0331) 5509-222  
christoph.meinel@hpi.uni-potsdam.de