Virtual platform of trust, a state of the art

Eléonore Hardy[1][0000-0002-6065-5856], Alexis Ulliac[1][0000-0001-7936-316X] and Paul Varela[1][0000-0001-9953-5360]

[1]Thales Secure Communications and Information Systems, 92230 Gennevilliers, France
firstname.lastname@thalesgroup.com

Abstract.

The use of virtualized and cloud environments has grown tremendously during the last decade and raised new threats. As privacy and security needs increased, the usage of a Trusted Platform Module (TPM) became trendier. This technology consisting of a passive crypto coprocessor installed on most of modern hardware helps to provide trust to users. Adapting TPM technology to a virtualized environment brings new security constraints and benefits. This paper presents a state of the art of the virtual TPM technology, how it can improve security and trust on virtualized environments. After an overall presentation of TPM and vTPM principles, this article presents specific architectures, security challenges and solutions. To finish, standardization initiatives are addressed before presenting a way forward at national level to enhance vTPM security for critical activities.

Keywords:
Protection, Virtual platform, TPM, trusted computing, Virtual TPM.