Secure Virtualization and Trusted Platform Management

There is a strong trend shift in the favor of adopting *virtualization* to get business benefits. The provisioning of virtualized enterprise resources is one kind of many possible scenarios. Where virtualization promises clear advantages it also poses new security challenges which need to be addressed to gain stakeholders confidence in the dynamics of new environment. One important facet of these challenges is establishing '*Trust'* which is a basic primitive for any viable business model. The Trusted computing group (TCG) offers technologies and mechanisms required to establish this trust in the target platforms. Moreover, TCG technologies enable protecting of sensitive data in rest and transit. We are exploring the applicability of these technologies to virtualize enterprise resources securely for provisioning, establish trust in the target platforms and securely manage these virtualized Trusted Platforms.

Key Concepts: Virtualization, Trusted Computing, Trust Management, Security Management