ORLANDO, Fla., Sept. 22, 2011 – Trusted Computing Group (TCG) today announced the release of the first Virtualized Platform Architecture, which describes how to build a trusted virtualized platform. With this specification, robust Trusted Computing technologies based on the TCG’s core concepts of the hardware root of trust can be added to existing virtual machine managers (VMMs), allowing virtual machines (VM) on the same platform to share hardware roots of trust.

A trusted virtual platform presents some unique challenges when compared to trusted physical platforms. These challenges occur when the Trusted Platform Module (TPM) is implemented in software in the VMM layer, but the TPM is still expected to provide the core security protections as if it was implemented in hardware. For example, all of the TPM’s private data may be present inside the VMM software layer creating the opportunity for customers to backup/restore the TPM or migrate the TPM to a new platform along with its VM. TPM migration and restore usages present some new potential threats that need to be addressed.

The new TCG Virtualized Trusted Platform Architecture Specification defines how a virtual TPM will behave and how it can be used with a physical TPM to allow remote parties to evaluate the level of trust offered by the overall platform (VM and its underlying VMM). The specification defines terminology, component features, and the virtualization layering design blueprint to ensure a common approach, as well as security requirements and implementation considerations for a TCG-compatible trusted platform. However, it does not specify how virtual or physical machines are specifically implemented by vendors.

“With the rapid adoption of virtualization in client and server systems, it’s time to incorporate Trusted Computing into this model to ensure that the software and trust properties of both the virtual and physical environments are the same,” notes Lee Wilson, chair, TCG Virtualized Platform Work Group and IBM. “Without the foundation of trust properties, virtualized systems with their software-based hypervisors remain vulnerable to a variety of attacks and will not offer the level of security required for enterprise and government computing.”

To get more information on the NSA Trusted Computing Conference and Exposition or to register, go to http://www.ncsi.com/nsatc11/index.html. TCG also has information and more details at http://www.trustedcomputinggroup.org/media_room/events/102.

**Trusted Computing Group**

The Trusted Computing Group (TCG) provides open standards that enable a safer computing environment across platforms and geographies. Benefits of Trusted Computing include protection of business-critical data and systems, secure authentication and strong protection of user identities, and the establishment of strong machine identity and network integrity. Organizations using built-in, widely available trusted hardware and applications reduce their total cost of ownership. TCG technologies also provide regulatory compliance that is based upon trustworthy hardware. More information and the organization’s specifications and work groups are available at the Trusted Computing Group’s website, [www.trustedcomputinggroup.org](http://www.trustedcomputinggroup.org). Follow TCG on [Twitter](http://www.twitter.com) and on [LinkedIn](http://www.linkedin.com).

-- 30 --

Brands and trademarks are the property of their respective owners.