Challenges for Trusted Computing

Ahmad-Reza Sadeghi

Horst Görtz Institute for IT Security, Ruhr-University Bochum
sadeghi@crypto.rub.de

The Trusted Computing Group (TCG), an alliance of a large number of IT enterprises, has published a set of specifications aiming at cost-efficient extensions of conventional computer architectures with security-related features and cryptographic mechanisms. The TCG core specification concerns the Trusted Platform Module (TPM) that acts as a root of trust of a computing platform and provides cryptographic primitives which can be used to realize more sophisticated security services. Currently, TPMs are implemented as dedicated chips mounted on the motherboard of a computer and many vendors already ship their platforms equipped with TPMs.

Trusted Computing (TC) is an emerging technology and several prominent research and industrial projects are investigating trustworthy IT systems based on TC with promising results. Nevertheless, for the employment in practice various challenging technical and research problems are still to be solved including:

TPM complexity: The TPM specification contains a large number of commands and parameters and seems unmanageable. A thorough analysis is still missing to determine the minimal/essential set of functionalities for the TPM.

TPM compliance: Recent efforts show that the majority of TPMs available on the market are non-compliant to the TCG specification. Currently, users of TCG-enabled platforms have no efficient means to test the trustworthiness of their TPM and/or its compliance.

Maintenance: Recovering sealed data and backups in case of modified platform configurations as well as the migration of TPM states among platforms (with possibly different trust level) demand for more satisfactory solutions.

Trust infrastructure: Distributed trusted computing needs an appropriate framework for handling trust in practice (platform certificates, trusted channels, attestation kernels, etc)

Attestation: Existing TCG attestation is not satisfactory and may need rethinking. In particular it discloses the system configuration raising privacy concerns. A more general concept is property-based attestation that requires attesting whether a computing platform (or an application) has the desired security properties instead of attesting measurements (hash values) of the corresponding binaries as proposed by the TCG. However, one still needs to define and efficiently determine reasonable properties.

Trustworthy systems demand for a careful design and security analysis of trusted computing components and their interfaces to provide multilateral security that is essential in multiparty computation scenarios in practice such as home banking, eGovernment, Grid computing, virtual data centers, etc.