Chapter 10
Trusted Computing for Collaboration

Joerg Abendroth
Technische Universität München, Germany

Holger Kinkelín
Technische Universität München, Germany

ABSTRACT

The term “trusted computing” refers to a technology developed by the Trusted Computing Group. It mainly addresses two questions: “Which software is executed on a remote computer?” and “How can secret keys and other security sensitive data be stored and used safely on a computer?”. In this chapter the authors introduce the ideas of the trusted computing technology first and later explain how it can help us with establishing “trust” into a business partner (e.g., for B2B or B2C interactions). More precisely: the authors explain how to establish trust into the business partner’s computing machinery. So in their chapter “trust” means, that one business partner can be sure, that the other business partner’s computing system behaves in an expected and non malicious manner. The authors define “trust” as something that can be measured by cryptographic functions on one computer and be reported towards and evaluated by the business partner’s computer, not as something that is derived from observations or built upon legal contracts.

INTRODUCTION

Collaboration in business environment requires trust. Often this trust is established by a legal framework, which is cumbersome and in case of computer interactions sometimes impossible. Trusted Computing aims to bridge this gap, but as the problem is hard, the solution is not a general one. One has to pay attention about the trust relationships and business models to benefit from the technology.

Other chapters in this book define trust as something that can be built up and achieved gradually over time and interactions. In this chapter trust is derived from cryptographic functions, integrity measurements of computer system components and credentials in signed certificates by known trusted parties.
The rest of the chapter first speaks about the basis of Trusted Computing, the history and scope of standardization, the required hardware and finally concepts. Then a section about the trust relationships in business environment opens the discussion on “Using Trusted Computing for Business”. Here the different collaboration types are shown and relevant business cases are outlined. Last thoughts on Trusted Computing for collaboration conclude the chapter.

About Trusted Computing

Ideas similar to Trusted Computing are almost as old as history in computing. E.g., in 1987 IBM developed the 4758 PCI Cryptographic Coprocessor, which was used in numerous research activities. Other research focused on securing the operating system itself.

Today operation systems are very complex, which makes them prone to errors. These errors often lead to exploits that can make critical calculations vulnerable for attacks. So it seems necessary to have a tamper-proof environment, e.g. a special chip, where critical calculations can be executed safely and secrets stored securely.

In 1999 the Trusted Computing Platform Alliance (TCPA), a first standardization organization to provide an interoperable standard for such a secure computing environment, was founded. The concepts of the TCPA where different to the current concepts of Trusted Computing standards and can best be characterized by including all components of a computing system. Today’s standards provide separate building blocks and leave out elements that could provide the ability of remotely controlling a device. While this scope is consumer friendly it introduces pitfalls in the area of business models, which will be discussed in the Section “Using Trusted Computing for Business”.

The Trusted Computing Group (TCG)

The Trusted Computing Group (TCG) is the standardization organization that defines open, vendor-neutral standards for Trusted Computing. The current so called “promoter members” are

- AMD
- Fujitsu Limited
- Hewlett-Packard
- IBM
- Infineon
- Intel Corporation
- Lenovo Holdings Limited
- Microsoft
- Seagate Technology
- Sun Microsystems, Inc.
- Wave Systems

There are further 131 companies that have a “contributor” or “adopter” membership, which points towards wide adoption of the technology and broad scope.

The TCG consists of several subgroups, namely:

- Authentication
- Hardcopy
- Infrastructure
- Mobile
- PC-Client
- Server
- (Trusted) Software Stack (TSS)
- Storage
- Trusted Network Connect (TNC)
- Trusted Platform Module (TPM)
- Virtualized Platform

In the following, some TCG subgroups will be introduced briefly. For a comprehensive introduction to the scope of all working groups the reader is kindly asked to visit the TCG website https://www.trustedcomputinggroup.org/groups/.