# Trusted Computing Platforms


Trusted Computing Platforms_下载链接1_

著者:Siani Pearson

出版者:Prentice Hall PTR

出版时间:2002-07-22

装帧:Hardcover

isbn:9780130092205

Preface February 2001 witnessed a major leap forward in the field of computer security with the publication of an innovative industry specification for "trusted platforms." This

heralded a new era in significantly higher security for electronic commerce and electronic interaction than currently exists. What's the difference between a "platform" and a "trusted platform"? A platform is any computing device-a PC, server, mobile phone, or any appliance capable of computing and communicating electronically with other platforms. A Trusted Platform is one containing a hardware-based subsystem devoted to maintaining trust and security between machines. Throughout this book, we use italics for terms like this that we are using in a very specific way. This industry standard in trusted platforms is backed by a broad spectrum of companies including HP, Compaq, IBM, Microsoft, Intel, and many others. Together, they form (or make up) the Trusted Computing Platform Alliance (TCPA). Major innovations in corporate security like this occur infrequently, but they are of great importance in affecting the development of the field for many years. In this book, we explain the new technology as simply as possible, why it has been developed, and how it will operate in the real world. In particular, this book aims to complement the TCPA standards by providing a plain-language primer of the technical specifications, as well as setting them in context and explaining how the technology will be used, both in the short term and in the longer term. Our hope is that the reader will gain a broad understanding of TCPA technology from a team who helped write the complex technical specification documents without having to read these documents "cold." It serves both as an ideal introduction to trusted computing for the general reader and as a method of improving the "learning curve" for manufacturers and application developers wishing to implement trusted systems. The book has a different approach to other descriptions of Trusted Platforms, being much more detailed and broad in context than the TCPA white papers and design philosophy document, yet avoiding the deep technical details of the TCPA specification. It is intended to explain, clarify, and inspire rather than specify. A lack of trust in electronic services is one of the major factors constraining the growth of e-commerce. The importance of secure interaction is widely appreciated, but many people are not up to date with the latest thinking and approaches. The radical new approach to trusted computing described here has the potential of liberating the sector and dictating the way electronic communication develops as the young century evolves. The problem addressed by the TCPA is that in modern information society, computer resources are becoming increasingly global and open. As a result, computing platforms are playing not only the role of computing devices, but also of communicating (connected) devices. Both local users and remote communicators could benefit from enhanced trust and confidence when using or communicating with computer platforms. Existing security technologies, such as user authentication and access control, cryptographic co-processors, and operating systems with different security services, are helpful in general but not suitable on their own for establishing the trust and confidence required. Computing security is a race between methods for constructing and breaching secure interaction. The TCPA has proposed a quantum leap in security, based on a novel but essentially straightforward concept. The TCPA has proposed a trusted computing platform solution based on tamper-resistant hardware physically located inside the platform. This tamper-resistant hardware provides the computer platform with a "root of trust," and it supports a new and important security feature, namely integrity challenge of the platform. The integrity challenge feature helps to build a chain of trust, which allows local and remote users to verify whether selected functions and resources of the computing platform have been installed and are operating in a way that satisfies them. At the time of this writing (2002), the first steps have already been made toward manufacture of Trusted Platforms. Several manufacturers have announced TPM-chip products. This book has been written to appeal to a wide audience. Different parts of the book are targeted to different types of readers and can be read in conjunction with the other parts or alone. There are four parts, each containing several chapters, as follows: Part 1 Introducing Trusted Platform Technology : This is the only part you need

to read if you just want an overview of what Trusted Platforms and TCPA are all about. It is for anyone who wishes to understand the difference between a Trusted Computer and a computer that includes conventional security features! This first part includes three chapters. Chapter 1 explains the basics of Trusted Platforms and their context. Chapter 2 gives examples of scenarios that are enabled by exploitation of the technology. Chapter 3 explains Trusted Platform technology itself in more detail, but still at a higher level than is addressed by the TCPA specification. Part 2 Trust Mechanisms in a Trusted Platform : This part is a companion to the TCPA specification. It gives a more detailed description of the most important features of TCPA technology than is given in Part 1, going to the functional description level for those who wish to understand the advantages and overheads of Trusted Platforms. Along with Part 1, this part is of interest to organizations engaged in legal, financial, and governmental activities or for any business in which trusted interaction in the virtual world is of great importance. Part 3 Trusted Platforms in Practice : This, along with Part 2, is particularly useful for those developers or technical people with a good understanding of security who are interested in using Trusted Platforms. Note that Chapter 11 is recommended reading for everyone. Part 4 Trusted Platforms for Organizations and Individuals : This part describes examples of the use of Trusted Platforms in organizational contexts, as well as their use by individuals. Appendices : Here, you'll find background material on the Trusted Computing Platform Alliance, the philosophy of trust, and basic cryptographic concepts. We have tried to make each part and each chapter self-contained, so you may find a certain amount of necessary repetition of information, for which we apologize. The book was written by a team of authors working on the same research project. It was edited by Siani Pearson. We would like to acknowledge some of the specific contributions by individual authors: Boris Balacheff to Parts 2 and 3 and technical review, Liqun Chen to Parts 2 and 4 and the appendices, Siani Pearson to Parts 1 and 4 and the appendices, David Plaquin to Part 3 and the book's figures, and Graeme Proudler to Parts 1 and 2 and general review.

作者介绍:

目录:

Trusted Computing Platforms_下载链接1_

## 标签

Tech

## 评论

---
Trusted Computing Platforms_下载链接1_

# 书评

---
Trusted Computing Platforms_下载链接1_