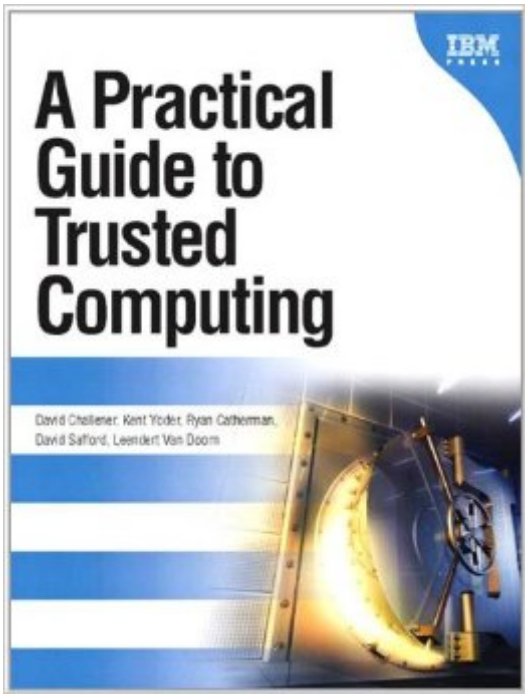
A Practical Guide To Trusted Computing (IBM Press)



Synopsis

Use Trusted Computing to Make PCs Safer, More Secure, and More Reliable Â Every year, computer security threats become more severe. Software alone can no longer adequately defend against them: whatâ ™s needed is secure hardware. The Trusted Platform Module (TPM) makes that possible by providing a complete, open industry standard for implementing trusted computing hardware subsystems in PCs. Already available from virtually every leading PC manufacturer, TPM gives software professionals powerful new ways to protect their customers. Now, thereâ ™s a start-to-finish guide for every software professional and security specialist who wants to utilize this breakthrough security technology. Â Authored by innovators who helped create TPM and implement its leading-edge products, this practical book covers all facets of TPM technology: what it can achieve, how it works, and how to write applications for it. The authors offer deep, real-world insights into both TPM and the Trusted Computing Group (TCG) Software Stack. Then, to demonstrate how TPM can solve many of todayâ ™s most challenging security problems, they present four start-to-finish case studies, each with extensive C-based code examples. Â Coverage includes What services and capabilities are provided by TPMs TPM device drivers: solutions for code running in BIOS, TSS stacks for new operating systems, and memory-constrained environments Using TPM to enhance the security of a PCâ ™s boot sequence Key management, in depth: key creation, storage, loading, migration, use, symmetric keys, and much more Linking PKCS#11 and TSS stacks to support applications with middleware services What you need to know about TPM and privacy--including how to avoid privacy problems Moving from TSS 1.1 to the new TSS 1.2 standard TPM and TSS command references and a complete function library Â

Book Information

File Size: 3454 KB

Print Length: 387 pages

Simultaneous Device Usage: Up to 5 simultaneous devices, per publisher limits

Publisher: IBM Press; 1 edition (December 27, 2007)

Publication Date: December 27, 2007

Sold by:Â Digital Services LLC

Language: English

ASIN: B004YW6M66

Text-to-Speech: Enabled

X-Ray: Not Enabled

Word Wise: Not Enabled

Lending: Not Enabled

Enhanced Typesetting: Not Enabled

Best Sellers Rank: #965,919 Paid in Kindle Store (See Top 100 Paid in Kindle Store) #183 inÂ Books > Computers & Technology > Hardware & DIY > Microprocessors & System Design > Embedded Systems #1318 inÂ Books > Computers & Technology > Networking & Cloud Computing > Network Security #3136 inÂ Books > Computers & Technology > Networking & Cloud Computing > Networks, Protocols & APIs

Customer Reviews

I think this book may be useful for people more familiar with the subject.I hoped to understand TPM command to encrypt/decrypt the data/key but find the book hard to read. There are several examples in C but those are evasive and leave me with more questions and doubt. I gave up after several chaptersTo be fair, I attempted to read TCG specs (and there are so many!) as well and those were equally confusing to me and it is difficult to satisfy all aspects of TPM. I have more understanding of TPM after reading several chapters but my original questions remained unanswered.

A decent general overview, but none of the example code seems to actually work. Is it for an older version? Who knows?

I have run into many people who have used this book and told me they had been lost trying to program the TPM until they found it. It tries to cover several things:What does the TPM do, and WHY?What is it appropriate to use the TPM to do?How can you program the TPM if:1) You need to talk to it at a low level2) If you need to write an application that uses it at a high level.There is a lot of C code in the book for examples.

Differential Equations and Boundary Value Problems: Computing and Modeling Guide to Literary Agents 2016: The Most Trusted Guide to Getting Published (Market) Children's Writer's & Illustrator's Market 2016: The Most Trusted Guide to Getting Published Novel & Short Story Writer's Market 2017: The Most Trusted Guide to Getting Published Writer's Market 2016: The Most Trusted Guide to Getting Published Poet's Market 2017: The Most Trusted Guide for Publishing Poetry Writer's Market Deluxe Edition 2016: The Most Trusted Guide to Getting Published 2015 Writer's Market: The Most Trusted Guide to Getting Published Computing: A Concise History (The MIT Press Essential Knowledge series) Stuck in the Shallow End: Education, Race, and Computing (MIT Press) Unlocking the Clubhouse: Women in Computing (MIT Press) DB2/Sql: A Professional Programmer's Guide (J Ranade Ibm Series) DB2/400: The New AS/400 Database: The Unabridged Guide to the New IBM Database Management System