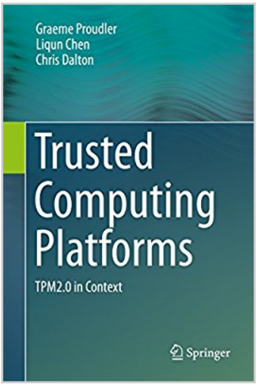

Trusted Computing Platforms: TPM2.0 in Context

By Graeme Proudler, Liqun Chen, Chris Dalton

Trusted Computing Platforms: TPM2.0 in Context By Graeme Proudler, Liqun Chen, Chris Dalton

In this book the authors first describe the background of trusted platforms and trusted computing and speculate about the future. They then describe the technical features and architectures of trusted platforms from several different perspectives, finally explaining second-generation TPMs, including a technical description intended to supplement the Trusted Computing Group's TPM2 specifications. The intended audience is IT managers and engineers and graduate students in information security.

Trusted Computing Platforms: TPM2.0 in Context

By Graeme Proudler, Liqun Chen, Chris Dalton

Trusted Computing Platforms: TPM2.0 in Context By Graeme Proudler, Liqun Chen, Chris Dalton

In this book the authors first describe the background of trusted platforms and trusted computing and speculate about the future. They then describe the technical features and architectures of trusted platforms from several different perspectives, finally explaining second-generation TPMs, including a technical description intended to supplement the Trusted Computing Group's TPM2 specifications. The intended audience is IT managers and engineers and graduate students in information security.

Trusted Computing Platforms: TPM2.0 in Context By Graeme Proudler, Liqun Chen, Chris Dalton Bibliography

- Rank: #1220069 in eBooks
- Published on: 2015-01-08
- Released on: 2015-01-08
- Format: Kindle eBook

Download and Read Free Online Trusted Computing Platforms: TPM2.0 in Context By Graeme Proudler, Liqun Chen, Chris Dalton

Editorial Review

From the Back Cover
In this book the authors first describe the background of trusted platforms and trusted computing, and speculate about the future. They then describe the technical features and architectures of trusted platforms from several different perspectives, finally explaining second-generation TPMs, including a technical description intended to supplement the Trusted Computing Group's TPM2 specifications. The intended audience is IT managers and engineers, and graduate students in information security.

About the Author

Graeme Proudler was a researcher at Hewlett-Packard Laboratories in Bristol, UK, and the Chair of the Trusted Computing Group’s Technical Committee until November 2013. He was the technical lead of the HP Labs research group that contributed to Trusted Computing Platform Alliance specifications, a founder member of the TCPA Technical Committee and original editor of the TCPA main (TPM) specification. His research interests include information security, networking and mobile communications.

Dr. Liqun Chen is a researcher at Hewlett-Packard Laboratories in Bristol, UK. She has developed a number of well-known cryptographic schemes, some of which were designed for and are implemented in the TPM. She has an extensive publication record in cryptography and information security and holds 38 granted US patents in these areas. She has served as editor or co-editor for five ISO/IEC standard documents in cryptography and serves on boards for related academic journals and conferences.

Christopher Dalton is a Principal Research Engineer within HP Labs, UK. His research interests include platform security (fixed and mobile), operating systems, network security and virtualisation, as well as a wider interest in distributed systems. He has been responsible for many successful technology transfers from research through to commercial products. He has published influential papers in the areas of systems, network security and virtualisation and has generated a number of patents in areas including novel low-level security features and efficient network virtualisation mechanisms.

Users Review

From reader reviews:

Lee Rutledge:

What do you think about book? It is just for students since they are still students or the item for all people in the world, what the best subject for that? Merely you can be answered for that query above. Every person has various personality and hobby for each other. Don't to be forced someone or something that they don't need do that. You must know how great and also important the book Trusted Computing Platforms: TPM2.0 in Context. All type of book is it possible to see on many options. You can look for the internet solutions or other social media.

Gregory Mackenzie:

The ability that you get from Trusted Computing Platforms: TPM2.0 in Context could be the more deep you searching the information that hide inside the words the more you get interested in reading it. It does not mean that this book is hard to know but Trusted Computing Platforms: TPM2.0 in Context giving you excitement feeling of reading. The writer conveys their point in certain way that can be understood by simply anyone who read the idea because the author of this e-book is well-known enough. This book also makes your own personal vocabulary increase well. It is therefore easy to understand then can go to you, both in printed or e-book style are available. We advise you for having this particular Trusted Computing Platforms: TPM2.0 in Context instantly.

Ann Edwards:

Hey guys, do you really wants to finds a new book to see? May be the book with the title Trusted Computing Platforms: TPM2.0 in Context suitable to you? Typically the book was written by well-known writer in this era. Often the book untitled Trusted Computing Platforms: TPM2.0 in Contextis a single of several books this everyone read now. This kind of book was inspired a number of people in the world. When you read this e-book you will enter the new shape that you ever know just before. The author explained their thought in the simple way, and so all of people can easily to be aware of the core of this book. This book will give you a great deal of information about this world now. To help you to see the represented of the world in this particular book.

Alberta Keyes:

That guide can make you to feel relax. This kind of book Trusted Computing Platforms: TPM2.0 in Context was colourful and of course has pictures on there. As we know that book Trusted Computing Platforms: TPM2.0 in Context has many kinds or style. Start from kids until youngsters. For example Naruto or Private investigator Conan you can read and believe that you are the character on there. Therefore not at all of book tend to be make you bored, any it makes you feel happy, fun and unwind. Try to choose the best book for you and try to like reading this.

Download and Read Online Trusted Computing Platforms: TPM2.0 in Context By Graeme Proudler, Liqun Chen, Chris Dalton #UB2QCEDFT5X

Read Trusted Computing Platforms: TPM2.0 in Context By Graeme Proudler, Liqun Chen, Chris Dalton for online ebook

Trusted Computing Platforms: TPM2.0 in Context By Graeme Proudler, Liqun Chen, Chris Dalton Free PDF d0wnl0ad, audio books, books to read, good books to read, cheap books, good books, online books, books online, book reviews epub, read books online, books to read online, online library, greatbooks to read, PDF best books to read, top books to read Trusted Computing Platforms: TPM2.0 in Context By Graeme Proudler, Liqun Chen, Chris Dalton books to read online.

Online Trusted Computing Platforms: TPM2.0 in Context By Graeme Proudler, Liqun Chen, Chris Dalton ebook PDF download

Trusted Computing Platforms: TPM2.0 in Context By Graeme Proudler, Liqun Chen, Chris Dalton Doc

Trusted Computing Platforms: TPM2.0 in Context By Graeme Proudler, Liqun Chen, Chris Dalton Mobipocket

Trusted Computing Platforms: TPM2.0 in Context By Graeme Proudler, Liqun Chen, Chris Dalton EPub

UB2QCEDFT5X: Trusted Computing Platforms: TPM2.0 in Context By Graeme Proudler, Liqun Chen, Chris Dalton