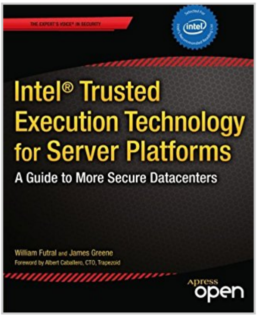
THE EXPERT'S VOICE® IN SECURITY
intel
Intel® Trusted Execution Technology for Server Platforms
A Guide to More Secure Datacenters
William Futral and James Greene
Foreword by Albert Caballero, CTO, Trapezoid
Apress open

Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security)

By William Futral, James Greene

Download Read Online

Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) By William Futral, James Greene

"This book is a must have resource guide for anyone who wants to ... implement TXT within their environments. I wish we had this guide when our engineering teams were implementing TXT on our solution platforms!”

John McAuley,EMC Corporation

"This book details innovative technology that provides significant benefit to both the cloud consumer and the cloud provider when working to meet the ever increasing requirements of trust and control in the cloud.”

Alex Rodriguez, Expedient Data Centers

"This book is an invaluable reference for understanding enhanced server security, and how to deploy and leverage computing environment trust to reduce supply chain risk.”

Pete Nicoletti. Virtustream Inc.

Intel® Trusted Execution Technology (Intel TXT) is a new security technology that started appearing on Intel server platforms in 2010. This book explains Intel Trusted Execution Technology for Servers, its purpose, application, advantages, and limitations. This book guides the server administrator / datacenter manager in enabling the technology as well as establishing a launch control policy that he can use to customize the server’s boot process to fit the datacenter’s requirements. This book explains how the OS (typically a Virtual Machine Monitor or Hypervisor) and supporting software can build on the secure facilities afforded by Intel TXT to provide additional security features and functions. It provides examples how the datacenter can create and use trusted pools.

With a foreword from Albert Caballero, the CTO at Trapezoid.

Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security)

By William Futral, James Greene

Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) By William Futral, James Greene

"This book is a must have resource guide for anyone who wants to ... implement TXT within their environments. I wish we had this guide when our engineering teams were implementing TXT on our solution platforms!”

John McAuley,EMC Corporation

"This book details innovative technology that provides significant benefit to both the cloud consumer and the cloud provider when working to meet the ever increasing requirements of trust and control in the cloud.”

Alex Rodriguez, Expedient Data Centers

"This book is an invaluable reference for understanding enhanced server security, and how to deploy and leverage computing environment trust to reduce supply chain risk.”

Pete Nicoletti. Virtustream Inc.

Intel® Trusted Execution Technology (Intel TXT) is a new security technology that started appearing on Intel server platforms in 2010. This book explains Intel Trusted Execution Technology for Servers, its purpose, application, advantages, and limitations. This book guides the server administrator / datacenter manager in enabling the technology as well as establishing a launch control policy that he can use to customize the server’s boot process to fit the datacenter’s requirements. This book explains how the OS (typically a Virtual Machine Monitor or Hypervisor) and supporting software can build on the secure facilities afforded by Intel TXT to provide additional security features and functions. It provides examples how the datacenter can create and use trusted pools.

With a foreword from Albert Caballero, the CTO at Trapezoid.

Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) By William Futral, James Greene Bibliography

- Sales Rank: #1427276 in Books
- Brand: imusti
- Published on: 2013-09-24
- Released on: 2013-11-22
- Original language: English
- Number of items: 1
- Dimensions: 9.25" h x .36" w x 7.50" l, .62 pounds
- Binding: Paperback
- 156 pages

Download and Read Free Online Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) By William Futral, James Greene

Editorial Review

Users Review

From reader reviews:

Charles Tapia:

In this 21st millennium, people become competitive in each way. By being competitive currently, people have do something to make these individuals survives, being in the middle of typically the crowded place and notice by simply surrounding. One thing that at times many people have underestimated that for a while is reading. Sure, by reading a e-book your ability to survive increase then having chance to stand up than other is high. For you personally who want to start reading some sort of book, we give you this specific Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) book as beginner and daily reading publication. Why, because this book is more than just a book.

Jessica Henriquez:

Do you among people who can't read gratifying if the sentence chained from the straightway, hold on guys this aren't like that. This Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) book is readable by means of you who hate the straight word style. You will find the data here are arrange for enjoyable reading experience without leaving actually decrease the knowledge that want to deliver to you. The writer involving Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) content conveys objective easily to understand by many individuals. The printed and e-book are not different in the written content but it just different as it. So , do you continue to thinking Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) is not loveable to be your top collection reading book?

Otis Key:

Reading a book to become new life style in this calendar year; every people loves to go through a book. When you read a book you can get a wide range of benefit. When you read guides, you can improve your knowledge, mainly because book has a lot of information in it. The information that you will get depend on what types of book that you have read. If you want to get information about your examine, you can read education books, but if you want to entertain yourself you can read a fiction books, these kinds of us novel, comics, and also soon. The Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) will give you a new experience in studying a book.

Jennifer Meeks:

That book can make you to feel relax. This particular book Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) was multi-colored and of course has pictures on the website. As we know that book Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) has many kinds or category. Start from kids until adolescents. For example Naruto or Investigator Conan you can read and believe you are the character on there. Therefore not at all of book are generally make you bored, any it makes you feel happy, fun and relax. Try to choose the best book for you personally and try to like reading that.

Download and Read Online Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) By William Futral, James Greene #R2TW0Q6ONXJ

Read Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) By William Futral, James Greene for online ebook

Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) By William Futral, James Greene 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 Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) By William Futral, James Greene books to read online.

Online Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) By William Futral, James Greene ebook PDF download

Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) By William Futral, James Greene Doc

Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) By William Futral, James Greene Mobipocket

Intel Trusted Execution Technology for Server Platforms: A Guide to More Secure Datacenters (Expert's Voice in Security) By William Futral, James Greene EPub