1. Record Nr. UNINA9910293151603321

Autore	Futral William
Titolo	Intel trusted execution technology for server platforms : a guide to more secure datacenters / / William Futral, James Greene ; foreword by Albert Caballero, CTO, Trapezoid
Pubbl/distr/stampa	Apress, 2013 New York : , : Apress, , 2013
ISBN	1-4302-6149-8
Edizione	[1st ed. 2013.]
Descrizione fisica	1 online resource (xx, 133 pages) : illustrations (chiefly color)
Collana	The expert's voice in security
Disciplina	004 005.74 005.8 005.82
Soggetti	Client/server computing - Security measures Database security Data encryption (Computer science)
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Chapter 1. Introduction to trust and Intel trusted execution technology -- Chapter 2. Fundamental principles of Intel TXT -- Chapter 3. Getting it to work : provisioning Intel TXT -- Chapter 4. Foundation for control : establishing launch control policy -- Chapter 5. Raising visibility for trust : the role of attestation -- Chapter 6. Trusted computing : opportunities in software -- Chapter 7. Creating a more secure datacenter and cloud -- Chapter 8. The future of trusted computing.
Sommario/riassunto	"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.