Contents at a Glance

Foreword xiii

About the Authors xv

Acknowledgments xvii

Introduction xix

■ Chapter 1: Introduction to Trust and Intel® Trusted Execution Technology 1

■ Chapter 2: Fundamental Principles of Intel® TXT 15

■ Chapter 3: Getting It to Work: Provisioning Intel® TXT 37

■ Chapter 4: Foundation for Control: Establishing Launch Control Policy 61

■ Chapter 5: Raising Visibility for Trust: The Role of Attestation 79

■ Chapter 6: Trusted Computing: Opportunities in Software 89

■ Chapter 7: Creating a More Secure Datacenter and Cloud 105

■ Chapter 8: The Future of Trusted Computing 119

Index 129

Contents

Foreword xiii

About the Authors xv

Acknowledgments xvii

Introduction xix

Chapter 1: Introduction to Trust and Intel Trusted Execution Technology 1

Why More Security? 2

Types of Attacks 2

What Is Trust? How Can Hardware Help? 3

What Is Intel Trusted Execution Technology? 4

Static Chain of Trust 5

Dynamic Chain of Trust 5

Virtualization 6

Measured Launch Environment 6

Finding Value in Trust 7

Cloud Computing 7

Attestation: The Founding Principle 8

Value to System Software 9

Cloud Service Provider/Cloud Service Client 10

What Intel TXT Does *Not* Do 11

Enhancements for Servers 11

Including BIOS in the TCB 11

Processor-Based CRTM 11

Trusting the SMM 12

Other Differences 12
Impact of the Differences 12
Roles and Responsibilities 12
OEM 12
Platform Owner 12
Host Operating System 13
Other Software 13
Chapter 2: Fundamental Principles of Intel TXT 15
What You Need: Definition of an Intel TXT–Capable System 15
Intel TXT–Capable Platform 16
Intel TXT Platform Components 16
The Role of the Trusted Platform Module (TPM) 18
TPM Interface 19
Random Number Generator (RNG) 20
SHA-1 Engine 21
RSA Engine and Key Generation 21
Platform Configuration Registers (PCRs) 21
Nonvolatile Storage 22
Attestation Identity Key (AIK) 23
TPM Ownership and Access Enforcement 23
Cryptography 23
Symmetric Encryption 24
Asymmetric Encryption 24
Cryptographic Hash Functions 24
Why It Works and What It Does 26
Key Concepts 26
Measurements 26
Secure Measurements 27
Static and Dynamic Measurements 27
The Intel TXT Boot Sequence 29

Measured Launch Process (Secure Launch) 31
Protection Against Reset Attacks 33
Launch Control Policy 33
Platform Configuration (PCONF) 34
Trusted OS Measurements (MLE Element) 34
Protecting Policies 35
Sealing 35
Attestation 35
Summary 36
Chapter 3: Getting It to Work: Provisioning Intel TXT 37
Provisioning a New Platform 37
BIOS Setup 38
Enable and Activate the Trusted Platform Module (TPM) 38
Enable Supporting Technology 38
Enabling Intel TXT 39
Summary of BIOS Setup 39
Automating BIOS Provisioning 40
Establish TPM Ownership 40
What Is TPM Ownership? Why Is This Important? 40
How to Establish TPM Ownership 40
Pass-Through TPM Model 41
Remote Pass-Through TPM Model 41
Management Server Model 42
Protecting Authorization Values 43
Install a Trusted Host Operating System 45
VMware ESXi Example 45
Linux Example (Ubuntu) 45
Create Platform Owner's Launch Control Policy 47
How It Works 47
What LCP Does 49

Why Is PO Policy Important? 55
Considerations 59
Summary 60
Chapter 4: Foundation for Control: Establishing Launch Control Policy 61
Quick Review of Launch Control Policy 61
When Is Launch Control Policy Needed? 63
Remote Attestation 63
What Does Launch Control Policy Deliver? 64
Platform Configuration (PCONF) Policy 64
Specifying Trusted Platform Configurations 65
Tools Needed for Creating a PCONF Policy 69
Difficulties with Using PCONF Policy 70
Specifying Trusted Host Operating Systems 71
Tools Needed for Creating MLE Policy 71
Options and Tradeoffs 72
Impact of SINIT Updates 72
Impact of Platform Configuration Change 73
Impact of a BIOS Update 73
Impact of OS/VMM Update 73
Managing Launch Control Policy 73
Think Big 73
Use a Signed List 74
Make Use of Vendor-Signed Policies 74
Use Multiple Lists for Version Control 74
Using the Simplest Policy 75
Other Tips 75
Strategies 75
Impact of Changing TPM Ownership 77
Decision Matrix 77

Chapter 5: Raising Visibility for Trust: The Role of Attestation 79

Attestation: What It Means 79

Attestation Service Components 80

Endpoint, Service, and Administrative Components 81

Attestation Service Component Capabilities 82

Administrative Component Capabilities 83

Attestation in the Intel TXT Use Models 83

Enabling the Market with Attestation 85

OpenAttestation 86

Mt. Wilson 87

How to Get Attestation 88

Chapter 6: Trusted Computing: Opportunities in Software 89

What Does "Enablement" Really Mean? 89

Platform Enablement: The Basics 91

Platform Enablement: Extended 93

Provisioning 94

Updates 94

Attestation 94

Reporting and Logging 95

Operating System and Hypervisor Enablement 95

Enablement at Management and Policy Layer 97

Provisioning 100

Updates 100

Attestation 100

Reporting and Logging 100

Enablement at the Security Applications Layer 101

Chapter 7: Creating a More Secure Datacenter and Cloud 105

When Datacenter Meets the Cloud 105

The Cloud Variants 106

Cloud Delivery Models 107

Intel TXT Use Models and the Cloud(s) 110
The Trusted Launch Model 110
Trusted Compute Pools: Driving the Market 112
Extended Trusted Pools: Asset Tags and Geotags 114
Compliance: Changing the Landscape 116
Chapter 8: The Future of Trusted Computing 119
Trust Is a Foundation 119
More Protections and Assurance 120
Is There Enough to Trust? 122
Measures at Launch Time 122
What Intel TXT Measures 123
The Whitelist Approach 123
The Evolution of Trust 123
Trusted Guest 124
End-to-End Trust 124
Runtime Trust 125
The Trust and Integrity "Stack" 125
Index 129