

Contents

1	Introduction — 1
1.1	Related Work — 2
1.1.1	Security Chip — 3
1.1.2	Trust within a Terminal Platform — 3
1.1.3	Trust between Platforms — 4
1.1.4	Trust in Network — 5
1.1.5	Test and Evaluation of Trusted Computing — 6
1.2	Our Work — 7
1.2.1	Chain of Trust — 8
1.2.2	Remote Attestation — 9
1.2.3	Trusted Network Connection — 12
1.2.4	Application of Trusted Computing — 13
1.2.5	Test and Evaluation of Trusted Computing — 15
1.3	Problems and Challenges — 16
1.4	Structure of This Book — 17
2	Trusted Platform Module — 18
2.1	Design Goals — 19
2.2	TPM Security Chip — 20
2.2.1	Introduction — 20
2.2.2	Platform Data Protection — 25
2.2.3	Identification — 29
2.2.4	Integrity Storage and Reporting — 31
2.2.5	Resource Protection — 33
2.2.6	Auxiliary Functions — 39
2.3	TCM Security Chip — 44
2.3.1	Main Functionalities — 44
2.3.2	Main Command Interfaces — 50
2.4	Mobile Trusted Module — 59
2.4.1	Main Features of MTM — 60
2.4.2	MTM Functionalities and Commands — 60
2.5	Developments of Related New Technologies — 62
2.5.1	Dynamic Root of Trust for Measurement — 63
2.5.2	Virtualization Technology — 64
2.6	Summary — 64
3	Building Chain of Trust — 66
3.1	Root of Trust — 67
3.1.1	Introduction of Root of Trust — 67
3.1.2	Root of Trust for Measurement — 67
3.1.3	Root of Trust for Storage and Reporting — 71

3.2	Chain of Trust — 72
3.2.1	The Proposal of Chain of Trust — 72
3.2.2	Categories of Chain of Trust — 73
3.2.3	Comparisons between Chains of Trust — 78
3.3	Systems Based on Static Chain of Trust — 79
3.3.1	Chain of Trust at Bootloader — 81
3.3.2	Chain of Trust in OS — 81
3.3.3	The ISCAS Chain of Trust — 86
3.4	Systems Based on Dynamic Chain of Trust — 94
3.4.1	Chain of Trust at Bootloader — 95
3.4.2	Chain of Trust in OS — 96
3.5	Chain of Trust for Virtualization Platforms — 98
3.6	Summary — 99
4	Trusted Software Stack — 100
4.1	TSS Architecture and Functions — 101
4.1.1	TSS Architecture — 101
4.1.2	Trusted Device Driver — 102
4.1.3	Trusted Device Driver Library — 103
4.1.4	Trusted Core Services — 104
4.1.5	Trusted Service Provider — 105
4.2	TSS Interface — 106
4.2.1	Object Type in TSM — 107
4.2.2	TDDL Interface in TSM — 108
4.2.3	TCS Interface in TSM — 109
4.2.4	TSP Interface in TSM — 112
4.3	Trusted Application Development — 119
4.3.1	Calling Method of Interfaces — 120
4.3.2	Example 1: File Encryption and Decryption — 121
4.3.3	Example 2: Signature Verification in DRM — 123
4.4	Open-Source TSS Implementation — 126
4.4.1	TrouSerS — 126
4.4.2	jTSS — 128
4.4.3	μTSS — 130
4.5	Summary — 132
5	Trusted Computing Platform — 133
5.1	Introduction — 133
5.1.1	Development and Present Status — 134
5.1.2	Basic Architecture — 135
5.2	Personal Computer — 136
5.2.1	Specification — 136
5.2.2	Products and Applications — 137

5.3	Server — 138
5.3.1	Specification — 139
5.3.2	Products and Applications — 140
5.4	Trusted Mobile Platform — 141
5.4.1	Specification — 141
5.4.2	Generalized Architecture — 142
5.4.3	Implementation of Trusted Mobile Platform — 145
5.4.4	Applications — 150
5.5	Virtualized Trusted Platform — 151
5.5.1	Requirements and Specification — 152
5.5.2	Generalized Architecture — 153
5.5.3	Implementation of Virtualized Trusted Platform — 154
5.5.4	Applications — 160
5.6	Applications of Trusted Computing Platform — 161
5.6.1	Data Protection — 161
5.6.2	Security Authentication — 162
5.6.3	System Security Enhancement — 163
5.6.4	Trusted Cloud Services — 163
5.6.5	Other Applications — 165
5.7	Summary — 166
6	Test and Evaluation of Trusted Computing — 168
6.1	Compliance Test for TPM/TCM Specifications — 168
6.1.1	Test Model — 169
6.1.2	Test Method — 175
6.1.3	Test Implementation — 178
6.2	Analysis of Security Mechanism of Trusted Computing — 180
6.2.1	Analysis Based on Model Checking — 180
6.2.2	Analysis Based on Theorem Proving — 183
6.3	Evaluation and Certification of Trusted Computing — 186
6.3.1	Common Criteria — 186
6.3.2	TPM and TNC Certification — 187
6.4	Comprehensive Test and Analysis System of Trusted Computing Platform — 187
6.4.1	Architecture and Functions of System — 188
6.4.2	Compliance Test for TPM/TCM Specification — 190
6.4.3	Tests of Cryptography Algorithms and Randoms — 191
6.4.4	Simulation of Security Chip and Protocol — 192
6.4.5	Promotion and Application — 193
6.5	Summary — 195
7	Remote Attestation — 197
7.1	Remote Attestation Principle — 198
7.1.1	Technology Foundation — 198

7.1.2	Protocol Model — 200
7.1.3	Interface Implementation — 201
7.2	Comparison of Remote Attestation Researches — 206
7.2.1	Attestation of Platform Identity — 207
7.2.2	Attestation of Platform Integrity — 208
7.3	Attestation of Platform Identity — 210
7.3.1	Attestation of Platform Identity Based on Privacy CA — 210
7.3.2	Direct Anonymous Attestation — 212
7.3.3	Research Prospects — 222
7.4	Attestation of Platform Integrity — 224
7.4.1	Binary Remote Attestation — 224
7.4.2	Property-Based Remote Attestation — 225
7.4.3	Research Prospects — 235
7.5	Remote Attestation System and Application — 235
7.5.1	Remote Attestation System in Security PC — 236
7.5.2	Integrity Verification Application on Mobile Platform — 239
7.5.3	Remote Attestation Integrated with the TLS Protocol — 240
7.6	Summary — 241

8 Trust Network Connection — 243

8.1	Background of TNC — 243
8.1.1	Introduction to NAC — 243
8.1.2	Commercial NAC Solutions — 245
8.1.3	Defects of Current Solutions and TNC Motivation — 248
8.2	Architecture and Principles of TNC — 249
8.2.1	Standard Architecture — 249
8.2.2	Overall Architecture — 249
8.2.3	Workflow — 253
8.2.4	The Advantages and Disadvantages of TNC — 254
8.3	Research on Extension of TNC — 255
8.3.1	Overview of the TNC Research — 255
8.3.2	Trust@FHH — 256
8.3.3	ISCAS Trusted Network Connection System — 258
8.4	Application of Trusted Network Connection — 262
8.5	Summary — 263

Appendix A: Foundations of Cryptography — 265

A.1	Block Cipher Algorithm — 265
A.1.1	AES — 265
A.1.2	SMS4 — 273
A.2	Public-Key Cryptography Algorithm — 275
A.2.1	RSA — 276
A.2.2	Elliptic Curve Public-Key Encryption Algorithm — 277

A.2.3	SM2 Public-Key Encryption Algorithm —	277
A.3	Digital Signature Algorithm —	278
A.3.1	ECDSA Digital Signature Algorithm —	279
A.3.2	SM2 Digital Signature —	280
A.4	Hash Function —	281
A.4.1	SHA-256 Hash Algorithm —	282
A.4.2	SM3 Hash Algorithm —	283
A.5	Key Exchange Protocols —	285
A.5.1	MQV Key Exchange Protocol —	286
A.5.2	SM2 Key Exchange Protocol —	287

References —	289
---------------------	------------

Index —	299
----------------	------------