

Contents

Preface	xvii
Acknowledgments	xxv
About the Authors	xxvii

Part I: Background Material **1**

Chapter 1 Introduction to Trusted Computing **3**

Computer Security Attacks Are Staggeringly Expensive	3
The Changing Threats to Computer Security	4
Vulnerable Programs	5
Malicious Programs: Viruses and Spyware/Adware	7
Misconfigured Programs	7
Social Engineering: Phishing and Pharming	7
Physical Theft of Data	8
Electronic Eavesdropping	8
Can Software Be Made Completely Secure?	9
How Can the TPM Help?	9
Privacy and Recovery—Special Considerations for Hardware	11
Summary	12
Endnotes	12

Chapter 2 Design Goals of the Trusted Platform Module **13**

Securely Reporting the Environment: Platform Status	14
Storing a Record of the Boot Sequence	14
Reporting the Boot Sequence Record	17
Secure Storage	18
Storing Data and Symmetric Keys	19
Storing Asymmetric Keys	19
Authorization	20

Secure Signatures	22
Secure Identity	23
Isolation of Users in a Multiple User Environment	23
Internal Random Number Generation	24
Features Not Included	25
Security Analysis	26
Summary	28
Chapter 3 An Overview of the Trusted Platform Module Capabilities	29
Secure Storage: The Storage Root Key	29
Migratable Versus Non-Migratable Keys	34
Types of Keys	35
Storage Keys	36
Binding Keys	36
Identity Keys	36
Signature Keys	36
Platform Integrity	37
Platform Configuration Registers	37
The Handoff Procedure	39
Maintenance	39
Secure Signatures	40
Avoiding Exposure	41
Privacy and Multiple Signatures	41
Summary	42
Part II: Programming Interfaces to TCG	43
Chapter 4 Writing a TPM Device Driver	45
TCG Device Driver Library	46
TPM 1.1b Specification Device Interface	47
Technical Details	47
Device Programming Interface	48
TPM 1.2 Specification Device Interface	50
Technical Details	51
Device Programming Interface	53
Summary	58
Chapter 5 Low-Level Software: Using BIOS and TDDL Directly	59
Talking to the TPM Through BIOS	59
Talking to the TPM Through TDDL	62
The IBM libtpm Package	62
Enabling and Clearing the TPM	63

Talking to the TPM	63
Getting Started with Some Simple TPM Commands	64
Taking Ownership	66
Creating and Using Keys	66
Checking the TPM Configuration	67
Summary	68
Chapter 6 Trusted Boot	69
Trusted Boot with Static Root of Trust	69
Dynamic Root of Trust Measurements	71
AMD's Secure Virtual Machine	72
Proof of Locality	75
Summary	76
Chapter 7 The TCG Software Stack	77
TSS Design Overview	77
The TCG Service Provider Interface (Tspi)	79
TSP Object Types	79
Context Objects	80
TPM Objects	81
Policy Objects	82
Key Objects	85
Encrypted Data Objects	87
Hash Objects	88
PCR Composite Objects	89
Non-Volatile Data Objects (TSS 1.2)	91
Migratable Data Objects (TSS 1.2)	92
Delegation Family Objects (TSS 1.2)	92
Direct Anonymous Attestation (DAA) Objects (TSS 1.2)	92
TSS Return Codes	93
TSS Memory Management	94
Portable Data	94
Persistent Key Storage	95
Signing and Verifying	97
Setting Callback Functions	99
The TSS Validation Data Structure	101
Summary	102
Chapter 8 Using TPM Keys	103
Creating a Key Hierarchy	103
Utility Functions	104
Summary	124

Chapter 9 Using Symmetric Keys	127
Data Binding	127
Sample Code	130
Data Sealing	132
Sample Code	133
Encrypting Files	136
Summary	138
Chapter 10 The TSS Core Service (TCS)	141
Overview of a TCS	141
How the TCS Manages Finite Resources	142
Further Abstracting the TCS Abstraction	144
Why a TCS Is Exposed Locally and Remotely	144
Utilizing and Implementing a TCS	145
Getting Started	145
Why WSDL Was Chosen	146
Brief Breakdown of the .wsdl File	147
The Header	147
The <types> Section	148
InParms and OutParms in the Complex Types	149
The Messages	150
The Operations in portType	150
The Operations in the Binding	151
The Service	151
Summary of the WSDL File	151
Using the WSDL File	151
The Ideal Situation	152
Example Using gSOAP	152
Using the gSOAP Stubs	153
Privacy Concerns with the TCS	154
Addressing Privacy	154
Grouping Desirable Functions	154
Summary	155
Chapter 11 Public Key Cryptography Standard #11	157
PKCS#11 Overview	158
A PKCS#11 TPM Token	158
RSA Key Types	158
RSA Key Restrictions	159
Administration	161
Design Requirements	162
openCryptoki's Design	162
Migration	169
Summary	178

127

127

130

132

133

136

138

141

141

142

144

144

145

145

146

147

147

148

149

150

150

151

151

151

151

152

152

153

154

154

154

155

#11 157

158

158

158

159

161

162

162

169

178

Part III: Architectures**179****Chapter 12 Trusted Computing and Secure Storage****181**

Linking to Symmetric Algorithms

181

Encrypting Files to Send to Someone Else on the Net Without a Public Key

183

Encrypting Files to Send to Someone Else on the Net with a Known Public Key

190

Encrypting Files for Storage on Your Hard Disk

191

Encrypting Files for Storage on a Group Hard Disk for Group Access

194

Encrypting Files for Storage in a Backup Facility

196

Locking Data to Specific PCs

198

Step 1

198

Step 2

199

Step 3

199

Step 4

199

Content Protection

200

Secure Printing

201

Intranet

201

Internet

202

Secure Faxing

202

Super Secure Migratable Storage

203

Summary

205

Chapter 13 Trusted Computing and Secure Identification**207**

Logon Password Storage

208

VPN Endpoints

208

Delegation of Authority

210

Delegation Without Allowing Further Migration

211

Credit Card Endpoints

211

Multiple Users on a Single System

213

Secure Hoteling

214

Creating a PKI with the Endorsement Key

216

Links to Biometrics

218

Links to Smart Cards

220

Smart Memory Cards and TPMs

220

Smart Signing Cards and TPMs

220

Virtual Dongles

221

Trusted Endpoints

221

Medical Solutions for HIPAA Compliance

222

COTS Security Solutions for the Military

225

Working with IP Telephony

226

Working with IPSec

226

Working with Service Meters

227

Working with Network Switches

228

Summary

230

Part III: Architectures 179

Chapter 12 Trusted Computing and Secure Storage 181

Linking to Symmetric Algorithms	181
Encrypting Files to Send to Someone Else on the Net Without a Public Key	183
Encrypting Files to Send to Someone Else on the Net with a Known Public Key	190
Encrypting Files for Storage on Your Hard Disk	191
Encrypting Files for Storage on a Group Hard Disk for Group Access	194
Encrypting Files for Storage in a Backup Facility	196
Locking Data to Specific PCs	198
Step 1	198
Step 2	199
Step 3	199
Step 4	199
Content Protection	200
Secure Printing	201
Intranet	201
Internet	202
Secure Faxing	202
Super Secure Migratable Storage	203
Summary	205

Chapter 13 Trusted Computing and Secure Identification 207

Logon Password Storage	208
VPN Endpoints	208
Delegation of Authority	210
Delegation Without Allowing Further Migration	211
Credit Card Endpoints	211
Multiple Users on a Single System	213
Secure Hoteling	214
Creating a PKI with the Endorsement Key	216
Links to Biometrics	218
Links to Smart Cards	220
Smart Memory Cards and TPMs	220
Smart Signing Cards and TPMs	220
Virtual Dongles	221
Trusted Endpoints	221
Medical Solutions for HIPAA Compliance	222
COTS Security Solutions for the Military	225
Working with IP Telephony	226
Working with IPSec	226
Working with Service Meters	227
Working with Network Switches	228
Summary	230

Chapter 14 Administration of Trusted Devices	231
Secure Backup/Maintenance	231
Assignment of Key Certificates	235
Secure Time Reporting	237
Key Recovery	239
TPM Tools	240
Summary	241
Chapter 15 Ancillary Hardware	243
Trusted Path	243
Special Keyboards	244
Trusted Display	246
Summary	247
Chapter 16 Moving from TSS 1.1 to TSS 1.2	249
Certified Migratable Keys	249
Commands	250
Tspi_TPM_CMKSetRestrictions	250
Tspi_Key_CMKCreateBlob	250
Tspi_Key_MigrateKey	251
Tspi_TPM_CMKApproveMA	252
Tspi_TPM_CMKCreateTicket	252
Tspi_Key_CMKConvertMigration	252
Delegation	253
Tspi_TPM_Delegate_AddFamily	255
Tspi_TPM_Delegate_GetFamily	256
Tspi_TPM_Delegate_InvalidateFamily	256
Tspi_TPM_Delegate_CreateDelegation	257
Tspi_TPM_Delegate_CacheOwnerDelegation	257
Tspi_TPM_Delegate_UpdateVerificationCount	258
Tspi_TPM_Delegate_VerifyDelegation	259
Tspi_TPM_Delegate_ReadTables	259
Direct Anonymous Attestation	260
Tspi_TPM_DAA_JoinInit	262
Tspi_TPM_DAA_JoinCreateDaaPubKey	263
Tspi_TPM_DAA_JoinStoreCredential	264
Tspi_TPM_DAA_Sign	264
Tspi_TPM_DAA_IssuerKeyVerification	265
Tspi_DAA_IssueSetup	265
Tspi_DAA_IssueInit	266
Tspi_TPM_DAA_VerifyInit	267
Tspi_TPM_DAA_VerifySignature	267
Tspi_TPM_DAA_RevokeSetup	268
Tspi_TPM_DAA_ARDecrypt	268

Locality	269
PCRs—New Behavior	269
NVRAM	270
Commands	271
Tspi_NV_DefineSpace	271
Tspi_NV_ReleaseSpace	271
Tspi_NV_WriteValue	272
Tspi_NV_ReadValue	272
Auditing Functions	273
Tspi_TPM_SetOrdinalAuditStatus	273
Tspi_TPM_GetAuditDigest	274
Monotonic Counter	275
Tspi_TPM_ReadCurrentCounter	275
Tick Counter	276
Tspi_TPM_ReadCurrentTicks	276
Tspi_TPM_TickStampBlob	277
SOAP	277
Transport Session	277
Tspi_Context_SetTransEncryptionKey	278
Tspi_Context_CloseSignTransport	278
Administrative and Convenience Functions	279
Commands	279
Tspi_TPM_CreateRevocableEndorsementKey	279
Tspi_TPM_RevokEndorsementKey	280
Tcsi_Admin_TSS_SessionPerlLocality	281
Tcsi_Admin_TSS_MaxTimePerlLocality	282
Tspi_TPM_CheckMaintenancePolicy	282
Tspi_Context_RegisterKey	283
Tspi_Context_UnregisterKey	284
Tspi_TPM_KeyControlOwner	284
Tcsi_EnumRegisteredKeys	285
Tspi_GetRegisteredKeyByUUID	285
Tspi_Context_GetRegisteredKeyByPublicInfo	286
Tspi_Context_GetRegisteredKeyByUUID	287
Tspi_Context_GetRegisteredKeyByUUID2	287
Tspi_EncodeDER_TsBlob	288
Tspi_DecodeBER_TsBlob	289
Example Program	289
Summary	290

Part IV: Appendixes	291
Appendix A TPM Command Reference	293
Appendix B TSS Command Reference	303
Appendix C Function Library	321
Appendix D TSS Functions Grouped by Object and API Level	323
Index	333