
Contents

Acknowledgments	xiii
Glossary and acronym expansions	xv
1 Introduction	1
1.1 About this book	1
1.1.1 The enterprise approach	1
1.1.2 User stories	2
1.2 What is trusted computing?	2
1.2.1 What do we mean by ‘trusted’?	3
1.2.2 A brief history of trusted computing	4
1.2.3 The Trusted Computing Group	4
1.3 TPMs at a high level	5
1.3.1 Roots of Trust	5
1.3.2 Chains of trust	7
1.3.3 The TPM threat model	7
1.3.4 What TPMs are good for	9
1.3.5 What TPMs aren’t good for	9
1.3.6 TPM versions	10
1.3.7 Common TPM myths	11
1.4 Where to find TPMs	14
1.5 TPM software options	15
2 When to use a TPM	17
2.1 Machine authentication examples	17
2.2 Data protection examples	18
2.3 Attestation examples	19
2.4 When not to use a TPM	20
2.4.1 When not to use: consumer DRM	20
2.4.2 When not to use: primary defence against physical threats	21
2.5 Complicating factors	21
2.5.1 Identifying TPMs	21
2.5.2 Enterprise PKI integration	22
2.5.3 Universal software support	23

3	TPM concepts and functionality	25
3.1	Ownership and authority	25
3.2	Root keys and primary seeds	26
3.2.1	TPM 1.2 root keys	27
3.2.2	TPM 2.0 primary seeds and hierarchies	27
3.3	Non-root keys	30
3.3.1	Root and non-root key relationships	31
3.3.2	Externally created keys and the TPM	32
3.4	Key certification	32
3.5	Roots of trust for measurement	32
3.6	Platform configuration registers	33
3.7	Quotes	34
3.8	NVRAM and key storage	35
3.9	Utility functions	35
3.10	Access control mechanisms	35
3.11	Cryptographic algorithms	36
3.12	Communicating securely with the TPM	36
3.13	The TPM in action	37
3.13.1	Possible TPM states	37
3.13.2	Reboots, and why they matter	37
3.13.3	Clearing: erasing your TPM	38
4	Programming introduction	39
4.1	TSS 1.2 code introduction	39
4.1.1	Categories of TSPI commands	42
4.1.2	TSS objects	43
4.1.3	Policies: providing passwords to the TPM	43
4.1.4	Object attributes	45
4.2	IBM TSS 2.0 code introduction	46
4.2.1	TPM 2.0 utilities sample code	48
4.2.2	File handling helper functions	48
5	Provisioning: getting the TPM ready to use	51
5.1	Provisioning: what it means, and why it matters	51
5.2	Basic steps of 1.2 TPM provisioning	51
5.2.1	Setting up a 1.2 TPM	52
5.2.2	Establishing trust in a 1.2 TPM	56
5.3	2.0 TPM provisioning and hierarchies	60
5.3.1	Changing hierarchy authorizations	61
5.3.2	Changing the hierarchy seeds	62
5.3.3	Creating primary keys and objects	62
5.4	Multiversion TPMs	63
5.5	TPM provisioning user stories	63
5.5.1	User stories: turning the TPM on	63
5.5.2	User stories: establishing trust in the TPM	64
5.5.3	User stories: taking ownership	66

5.6	Remote verification of TPM keys	67
5.6.1	Certification: 1.2 TPM keys and PKI	67
5.6.2	Certification: the homegrown approach	68
5.7	Provisioning-time key certification user stories	69
6	First steps: TPM keys	71
6.1	TPM keys	71
6.1.1	Advantages and disadvantages of TPM keys	71
6.2	The basic types of TPM keys	72
6.2.1	TPM 1.2 key types	72
6.2.2	TPM 2.0 key attributes	74
6.3	Authorization options for TPM keys	75
6.4	Creating TPM keys	75
6.4.1	Parent keys	75
6.4.2	Key creation commands	77
6.5	Key creation user stories	82
6.6	Migratable and duplicatable keys	83
6.6.1	1.2 Normal migratable keys	83
6.6.2	1.2 Certifiable Migration Keys	87
6.6.3	2.0 Duplicatable keys	91
6.6.4	When to use migratable or duplicatable keys	93
6.7	Migratable key user stories	93
6.8	Loading TPM keys	94
6.8.1	Additional loading features in 2.0	95
6.9	Handles, names, and authorization: using TPM keys in other commands	95
6.9.1	Key handles and security	95
6.9.2	Pre-defined handles	96
6.10	Authorization sessions	97
6.11	Certifying TPM keys	98
6.11.1	TPM 1.2: certifying identity keys	100
6.11.2	Certifying other TPM keys (1.2 and 2.0)	102
6.11.3	Retrieving public portions of TPM keys	105
6.12	Using keys created outside the TPM	107
6.13	The TPM's access control models	108
6.13.1	Physical presence	108
6.13.2	TPM 1.2: user authentication, PCRs, and localities	109
6.13.3	TPM 2.0's Enhanced Authorization	110
6.14	Key access control user stories	114
6.15	TSS 1.2 key management code examples	116
6.15.1	Background: using the SRK	116
6.15.2	Key creation	116
6.15.3	Creating identity keys	119
6.15.4	Key loading	121
6.15.5	Using public keys	123

6.16	TSS 2.0 key management code examples	125
6.16.1	Key creation	125
6.16.2	Key loading	128
6.16.3	Using public keys	129
6.16.4	Enhanced Authorization policies	130
7	Machine authentication	137
7.1	What is machine authentication?	137
7.1.1	Signing versus encryption	137
7.1.2	The limits of TPM-based machine authentication	138
7.1.3	What about user authentication?	138
7.2	Signing-based machine authentication	139
7.2.1	How it works	139
7.2.2	When to use it	140
7.2.3	The TPM and signing-based authentication	141
7.2.4	Nonces: why they matter and how to use them	144
7.2.5	Mitigating man-in-the-middle attacks	146
7.3	Encryption-based machine authentication	147
7.3.1	How it works	147
7.3.2	When to use it	149
7.4	User identification versus machine authentication	150
7.5	Machine authentication user stories	151
7.6	1.2 TSS machine authentication code examples	153
7.6.1	Setting a signature scheme	153
7.6.2	Signing and verifying hashed data	154
7.6.3	Encryption and decryption	154
7.7	TSS 2.0 machine authentication code examples	154
7.7.1	Signing	154
7.7.2	Verifying signatures	156
7.7.3	Encryption and decryption	157
8	Data protection	159
8.1	The pros and cons of TPMs for data storage	159
8.2	Basic TPM encryption features	161
8.2.1	Storage hierarchies and data protection	162
8.3	Disk encryption, bulk data protection, and secure backups	163
8.4	Small-scale data protection	163
8.4.1	Small-scale local encryption	164
8.5	Secure data transmission	166
8.5.1	Binding, legacy keys, and backwards compatibility	168
8.6	Alternate backup techniques	168
8.7	The TPM's internal storage (NVRAM)	168
8.7.1	Using NVRAM in 1.2	170
8.7.2	Using NVRAM in 2.0	171

8.8	Conditional data access	175
8.9	Data protection user stories	176
8.10	TSS 1.2 data protection code examples	179
8.10.1	Binding and unbinding	179
8.10.2	Sealing and unsealing	180
8.10.3	Using NVRAM	181
8.11	TSS 2.0 data protection code examples	184
8.11.1	Creating a sealed blob	184
8.11.2	Decrypting a sealed blob	186
8.11.3	Using NV storage	186
8.11.4	Reading NV contents and manufacturer certificates	190
9	Attestation	193
9.1	Machine state and the TPM	193
9.1.1	Measurement chains of trust	193
9.1.2	The Static Root of Trust for Measurement	194
9.1.3	The Dynamic Root of Trust for Measurement	195
9.2	Using the PCRs	200
9.2.1	Essential PCR operations	200
9.2.2	Measurement and PCRs	202
9.2.3	Beyond measurements: creative uses of PCRs	204
9.2.4	1.2 PCR design	206
9.2.5	2.0 PCR design	207
9.2.6	Choosing PCRs to use	209
9.2.7	PCRs beyond the PC	210
9.3	Basic attestation techniques	211
9.3.1	Quotes	211
9.3.2	Verifying quotes	214
9.3.3	Constrained key attestation	216
9.3.4	Direct anonymous attestation	216
9.4	Machine state measurement in theory and reality	221
9.5	Attestation user stories	221
9.6	TSS 1.2 attestation code examples	225
9.6.1	Reading PCR contents	225
9.6.2	Extending PCRs	225
9.6.3	Resetting PCRs	226
9.6.4	Creating and verifying a quote	227
9.7	TSS 2.0 attestation code examples	232
9.7.1	Creating a PCR selection	232
9.7.2	Reading PCR contents	233
9.7.3	Extending PCRs	233
9.7.4	Resetting PCRs	234
9.7.5	Creating and verifying quotes	235

10 Other TPM features	237
10.1 The smorgasbord	237
10.2 Clearing the TPM	237
10.2.1 Revoking trust in an EK	239
10.2.2 Clearing user stories	239
10.3 Random number generation	239
10.3.1 Random number user stories	240
10.4 TPM configuration	241
10.4.1 Configuration in 1.2	241
10.4.2 Configuration in 2.0	242
10.4.3 Configuration user stories	247
10.5 Monotonic counters	248
10.5.1 Monotonic counter user stories	249
10.6 Storing extra keys in the TPM	250
10.6.1 Persistent key user stories	251
10.7 Command auditing	252
10.7.1 Command audit user stories	254
10.8 Field upgrades	254
10.9 1.2-exclusive features	255
10.9.1 Temporarily deactivating the TPM	255
10.9.2 Maintenance archives	255
10.9.3 Delegation	257
10.9.4 Tickstamps	260
10.10 2.0-exclusive features	262
10.10.1 Cryptographic primitives	262
10.10.2 Clocks and attesting to local time	265
 11 Software, specifications, and more: Where to find other TPM resources	 269
11.1 1.2 Programming tools	269
11.1.1 1.2 Trusted/TCG software stacks (TSS)	269
11.1.2 Microsoft's TBS	270
11.2 2.0 Programming tools	270
11.2.1 IBM TSS 2.0	270
11.2.2 2.0 TSS.Net and TSS.C++	271
11.3 Books, courses, and other digested material	271
11.3.1 TPM 1.2 concepts	271
11.3.2 TPM 1.2 programming	271
11.3.3 TPM 2.0	272
11.3.4 Other trusted computing topics	272
11.4 Community	273
11.4.1 The TCG	273
11.4.2 TrouSerS-users mailing list	273

11.5	1.2 Specifications	274
11.5.1	1.2 TSS specification	274
11.5.2	1.2 TPM specification	276
11.6	2.0 Specifications	279
11.6.1	TCG TSS (TPM Software Stack) specifications	279
11.6.2	2.0 TPM specifications	281
11.6.3	2.0 Supporting specifications	283
11.7	Platform specifications	285
11.7.1	1.2 Platform specifications	285
11.7.2	2.0 Platform specification	286
11.7.3	Specifications applying to multiple TPM versions	286
11.8	Other useful resources	286
11.8.1	The <code>tpm-tools</code> package	286
11.8.2	TPM manufacturers	287
11.8.3	TPM 2.0 simulators	287
11.8.4	Example open-source applications	288
11.8.5	Useful trusted computing tools	289
11.9	Commercial software	289
12	Troubleshooting	291
12.1	When all else fails	291
12.2	There's no TPM in the BIOS menu	291
12.3	Trouble getting any software working	292
12.3.1	Linux-specific tips	292
12.4	TPM returning errors	292
12.5	TSS 1.2 code returning errors	293
12.6	Problems using TPM data structures	294
13	Conclusion and review	295
13.1	What the TPM is good for	295
13.2	Common TPM use cases	295
13.3	The potential (and peril) of the future	296
13.4	In conclusion	296
Appendix A	Basic cryptographic concepts	299
A.1	The limitations of this appendix	299
A.2	Basic vocabulary	299
A.3	Symmetric cryptography	299
A.4	Asymmetric (public key) cryptography	300
A.5	Key derivation functions	301
A.6	Hashes	301
A.6.1	HMACs	301
A.7	Nonces	302
A.8	Zero-knowledge proofs	302

Appendix B	Command equivalence and requirements charts	305
B.1	Key	305
B.2	TPM 1.2 command equivalence and requirements	306
B.3	TPM 2.0 command requirements	312
Appendix C	Complete code samples	317
C.1	1.2 TSS code samples	317
C.1.1	Sealing and unsealing	317
C.1.2	Using NVRAM	321
C.2	2.0 TSS code samples	324
C.2.1	Creating objects	324
C.2.2	Retrieving the TPM's internal time	342
Copyright Notices		351
Index		353