

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	The State of Play	2
1.2	Objectives	4
1.3	Trusted Computing Technology	6
1.4	Benefits of Trusted Computing	7
1.5	Trust, Instead of Security	9
1.5.1	Secure Computing	9
1.5.2	Trusted Computing	10
1.6	Limitations of Trusted Computing	12
1.7	Concerns About Trusted Computing	13
1.8	First Generation Trusted Computing	18
	References	19
<b>2</b>	<b>Futures for Trusted Computing</b>	<b>21</b>
2.1	Trusted Virtualisation	21
2.1.1	Privacy Implications of Trusted Virtualisation	24
2.1.2	Virtualised Trusted Platforms	25
2.2	Future Trusted Services	26
2.2.1	Data Deletion	26
2.2.2	Contracts and Negotiations	27
2.2.3	Single Sign-On	28
2.2.4	Trusted Software Agents	28
2.2.5	What You See Is What You Sign	29
2.3	Infrastructure Requirements	29
2.3.1	Public Key Infrastructure	29
2.3.2	Manufacture	30
2.3.3	Upgrading TPMs	31
2.3.4	Upgrading Integrity Metrics	31
2.3.5	Auditing Trusted Platforms	32
2.3.6	Discovering Trusted Services	33

<b>3</b>	<b>Basics of Trusted Platforms . . . . .</b>	<b>37</b>
3.1	Design Constraints, Requirements, and Motivations . . . . .	37
3.1.1	Legacy Platforms, Software and Infrastructure . . . . .	37
3.1.2	Out of the Box . . . . .	38
3.1.3	Legal . . . . .	38
3.1.4	Privacy Constraints . . . . .	40
3.1.5	Disaster Recovery . . . . .	41
3.2	Conventional Security in Trusted Platforms . . . . .	43
3.2.1	High Security . . . . .	44
3.2.2	No Global Secrets . . . . .	45
3.2.3	Separation of Privilege . . . . .	45
3.2.4	Authorisation and Authentication of the Owner and User . . . . .	46
3.2.5	Dictionary Attacks . . . . .	48
3.2.6	Cryptographic Algorithms . . . . .	49
3.2.7	Isolation of Processes . . . . .	50
3.2.8	Certification . . . . .	51
3.3	Innovations in Trusted Platforms . . . . .	57
3.3.1	General Principles . . . . .	59
3.3.2	Roots of Trust . . . . .	61
3.3.3	Platform Configuration Registers . . . . .	66
3.3.4	Authenticated/Measured Boot . . . . .	66
3.3.5	Authenticated/Measured Secure Boot . . . . .	67
3.3.6	Protected Storage, Data Backup and Recovery . . . . .	67
3.3.7	Attestation . . . . .	72
3.3.8	Physical Presence and Provisioning Authorisation . . . . .	74
3.3.9	Recognising and Identifying a Trusted Platform . . . . .	77
3.4	Types of Trusted Platform . . . . .	84
3.4.1	Personal Computers . . . . .	84
3.4.2	Servers and Data Centres . . . . .	86
3.4.3	Mobile Phones . . . . .	86
3.4.4	Appliances . . . . .	91
3.5	Trusted Platform Lifecycle . . . . .	92
3.5.1	TPM Design . . . . .	92
3.5.2	TPM Manufacture . . . . .	93
3.5.3	Platform Manufacture . . . . .	96
3.5.4	Platform Deployment . . . . .	98
3.5.5	Platform Use . . . . .	101
3.5.6	Platform Maintenance and Recovery . . . . .	102
3.5.7	Platform Redeployment . . . . .	105
3.5.8	TPM and Platform Revocation . . . . .	105
3.5.9	Platform Decommissioning . . . . .	106
	References . . . . .	106

<b>4</b>	<b>Trusted Platform Architecture</b>	109
4.1	Isolation	110
4.1.1	Isolation Hardware	111
4.2	Credentials	112
4.3	Chain of Trust	112
4.4	Integrity Metrics	115
4.5	Platform Configuration Registers	116
4.6	Audit	118
4.7	Verifying the State of a Trusted Platform	118
4.8	Trusted Platform Module	119
4.9	Locality	122
4.10	Peripherals	123
4.10.1	Trusted Drives	123
4.11	TPM Software Interface	124
4.12	Virtualisation	126
4.12.1	Hosts of Virtualised Trusted Platforms	127
4.12.2	Virtualised Trusted Platforms	127
4.12.3	TPM Virtualisation	128
	References	129
<b>5</b>	<b>TPM2 Requirements</b>	131
5.1	Controllability and Privacy	131
5.1.1	Controllability	132
5.1.2	Privacy	135
5.2	Protecting the Platform's Services	135
5.3	Cryptographic Agility	136
5.4	The Commercial Environment	139
5.5	What Works, and What Doesn't Work	140
5.6	What's Unpopular	142
5.7	Platform Manufacturer Requirements	143
5.8	Hypervisor and OS Enhancements	147
5.9	Other Considerations	149
	Reference	150
<b>6</b>	<b>TPM2 Operation</b>	151
6.1	TPM2 and Its Host Platform	155
6.2	Using TPM2 Instead of TPMv1.2	157
<b>7</b>	<b>Initialising TPM2</b>	173
7.1	Manufacture	173
7.1.1	Providing TPM Endorsement	173
7.1.2	Providing Platform Credentials	175
7.1.3	Providing a Trusted Computing Base	175
7.1.4	TCB Authorisation Requirements	177
7.1.5	Storing TCB Keys in the TPM	178

7.1.6	Storing TCB data in the TPM . . . . .	179
7.1.7	Provisioning Platform Configuration Registers . . . . .	181
7.1.8	Allowing “Physical Presence” Authorisation . . . . .	183
7.2	Booting the Platform . . . . .	184
7.2.1	Initialising the TPM . . . . .	184
7.2.2	Ensuring that the Primary TCB can Manage the TPM . . . . .	186
7.2.3	Testing the TPM . . . . .	187
7.2.4	Using the TPM to Assist the TCB . . . . .	187
7.2.5	Enabling the Customer to Control the TPM via the Primary TCB . . . . .	188
7.2.6	Enabling or Disabling Further Access to the TPM . . . . .	189
7.3	Recording Platform History in PCRs . . . . .	189
7.4	Run-Time Initialisation . . . . .	192
7.5	Late Launch Environments . . . . .	193
<b>8</b>	<b>Managing TPM2 . . . . .</b>	<b>197</b>
8.1	Obtaining Management Information . . . . .	197
8.2	Keeping TPM Data Outside the TPM . . . . .	200
8.2.1	Short-Term Cached TPM Data . . . . .	204
8.2.2	Long-Term Cached TPM Data . . . . .	209
8.3	Dictionary Attacks . . . . .	214
8.4	Auditing Commands . . . . .	218
8.5	Clock and Timer . . . . .	221
8.5.1	Clock Functionality . . . . .	221
8.5.2	Timer Functionality . . . . .	222
8.6	Platform Shutdown . . . . .	222
<b>9</b>	<b>Accessing Keys and Data in TPM2 . . . . .</b>	<b>225</b>
9.1	Names and QualifiedNames . . . . .	225
9.2	Session Basics . . . . .	226
9.3	HMAC Sessions . . . . .	228
9.3.1	Freshness Nonces in HMAC Sessions . . . . .	228
9.3.2	Binding and Salting HMAC Sessions . . . . .	229
9.3.3	SessionKeys in HMAC Sessions . . . . .	230
9.3.4	HMAC Checksums on Commands and Responses . . . . .	231
9.3.5	Encrypting Command Parameters and Response Parameters . . . . .	232
9.3.6	Auditing HMAC Sessions . . . . .	233
9.4	Authorisation Roles . . . . .	235
9.5	Authorisation Session Types . . . . .	236
9.6	Plain Authorisation . . . . .	238
9.6.1	Plain Authorisation Without a Session . . . . .	239
9.6.2	Plain Authorisation with HMAC Sessions . . . . .	239

9.7	Policy Authorisation . . . . .	240
9.7.1	Composing a Policy . . . . .	240
9.7.2	Enumerating a Policy . . . . .	249
9.7.3	Assigning a Policy . . . . .	252
9.7.4	Executing a Policy . . . . .	252
<b>10</b>	<b>Customer Configuration of TPM2 and Its Host Platform . . . . .</b>	<b>255</b>
10.1	Customer Responsibilities . . . . .	255
10.2	Provisioning . . . . .	257
10.3	Setting up NV Storage . . . . .	260
10.4	Assigning Physical Presence Gating to Commands . . . . .	264
10.5	Assigning Personal Endorsement Keys . . . . .	265
10.6	Assigning Platform Identities . . . . .	267
10.6.1	Identities with Some Privacy Risk but Low Complexity . . . . .	268
10.6.2	Identities with Intermediate Privacy Risk, but Intermediate Complexity . . . . .	270
10.6.3	Identities with No Known Privacy Risk, but Higher Complexity . . . . .	273
	Reference . . . . .	275
<b>11</b>	<b>Starting to Use TPM2 . . . . .</b>	<b>277</b>
11.1	Testing TPM2 . . . . .	278
11.2	Creating and Obtaining Random Numbers . . . . .	279
11.3	Starting a Key Hierarchy . . . . .	279
11.4	Populating a Key Hierarchy by Creating Keys . . . . .	284
11.5	Populating a Key Hierarchy by Importing Keys . . . . .	290
11.6	Making a Key from an External Hierarchy Ready for Use . . . .	290
11.7	Making an External Public Key or Plaintext Key Ready for Use . . . . .	291
11.8	Duplicating a Key . . . . .	292
11.9	Embedding and Ejecting Keys . . . . .	294
11.10	Reading the Public Part of a Loaded Key . . . . .	295
11.11	Changing Authorisation Values . . . . .	295
11.12	Encrypting and Sealing Data . . . . .	297
11.13	Decrypting Data and Unsealing Data . . . . .	300
11.14	Signing . . . . .	301
11.15	Verifying Signatures . . . . .	304
11.16	Obtaining PCR Values . . . . .	305
11.17	Certifying Key Creation . . . . .	309
11.18	Cross Certification of Keys . . . . .	314
11.19	Certifying Sequences of Commands . . . . .	319
11.20	Certifying the Usage of Commands . . . . .	322
11.21	Certifying TPM Time, Resets, and TPM Firmware Version . . .	326
11.22	Storing Data in NV Storage . . . . .	330

11.23	Certifying NV Storage . . . . .	333
11.24	Using TPM2 as an Ordinary Cryptographic Service . . . . .	337
<b>12</b>	<b>Direct Anonymous Attestation (DAA) in More Depth . . . . .</b>	<b>339</b>
12.1	The Concept of General Anonymous Digital Signatures . . . . .	339
12.2	The Concept of DAA . . . . .	341
12.3	The Setup Algorithm . . . . .	343
12.4	The DAA Join Protocol . . . . .	344
12.5	The Sign/Verify Protocol . . . . .	346
12.6	The Link Algorithm . . . . .	348
12.7	Revocation Considerations . . . . .	348
12.8	Discussion on DAA Security Levels . . . . .	350
	References . . . . .	351
<b>13</b>	<b>Machine Virtualisation, Virtual Machines, and TPMs . . . . .</b>	<b>353</b>
13.1	Introduction . . . . .	353
13.2	Machine Virtualisation and Security . . . . .	354
13.3	Containment and Isolation . . . . .	354
13.4	Robust Control and Introspection Point . . . . .	355
13.5	Small Code Base . . . . .	355
13.6	Examples of Hypervisor-Based Enhanced Security . . . . .	356
	13.6.1 The TPM and Supporting Machine Virtualisation . . .	357
	13.6.2 Additional Chipset and CPU Hardware Extensions . . .	358
	13.6.3 Machine Virtualisation and Supporting the TPM . . .	359
	13.6.4 Challenges Around TPM and Virtualisation . . . . .	360
	13.6.5 Summary . . . . .	360
	References . . . . .	360
	<b>Index . . . . .</b>	<b>361</b>

Trusted Computing Platforms

TPM2.0 in Context

Proudler, G.; Chen, L.; Dalton, C.

2014, XVIII, 382 p. 9 illus., 2 illus. in color., Hardcover

ISBN: 978-3-319-08743-6