

# Contents

---

## **Chapter 1 Trusted Computing 1**

The Basic Problem of Trust 2

Basic Definitions 3

    Our Definition of Trust 3

    The Trust Decision 4

    The Platform 7

    The Client 7

    Owner, User, and Operator 7

    Building Blocks 8

    Trusted versus Trustable 9

The Weakest Link 9

    Protection in the Enclave 12

    Effect of Providing More Protections 12

    Joining an Enclave 12

The Basic Trusted Computer 13

Basic Cryptography 14

    Symmetric Encryption 14

    Asymmetric Encryption 15

    Combination 15

    Cryptographic Hash 16

Trusted Channel and Trusted Path 16

    Trusted Channel 16

    Trusted Path 16

- Combination 17
- The Data Life Cycle 17
  - Execute Phase 17
  - Move Phase 18
  - Store Phase 19

## **Chapter 2 History of Trusted Computing 21**

- Early Papers 22
  - 1970 Task Force 22
  - Bell-LaPadula 25
  - The Rainbow Series 25
  - Industry Response 26
- The Future through the Past 27
- Personal Computers 28
- CPU Internals 30
  - Protected Mode 30
  - Memory Management 31
  - Front-side Bus 33
  - Multiple CPU Systems 33
- MCH 34
  - Memory 34
  - Display Adapter 34
- ICH 34
  - Keyboard 34
  - USB 35
  - LPC Bus 35
- Current Intel® Architecture Security Support 35
  - Rings 35
  - Protected Mode 36
  - Paging 36
- Security Properties 37

## **Chapter 3 The Current Environment 37**

- Platform 38
- Hardware 38
- Operating System 39
  - Ring Use 39
  - Drivers 40
  - Configuration 41
- Applications 41
  - Installation 41

- Drivers 42
- Configuration 42
- Malware 42
  - Malware Components 42
  - Break Once, Run Everywhere 43
- Configurations 44
- Finding Bad Platforms 44

## **Chapter 4 Anatomy of an Attack 45**

- Programmer versus Attacker 47
- Application Today 48
  - Application Components 49
  - Display Windows 49
  - Reading Keystrokes 50
  - Password Processing 50
  - Program Decision 51
- Malware Attack Points 51
  - Manipulate Memory 52
  - Manipulate Input 53
  - Manipulate Output 55
- Attack Overview 56
- Mitigating Attacks 57
  - Hardware Mitigations 58

## **Chapter 5 Elemental Groups 59**

- Element Purpose 60
- Trusted Platform Elements 60
- Element Groups 61
  - System Protections 63
  - Physical Hardware 64
  - Between Partitions 64
  - Outside 64
  - Inside 65

## **Chapter 6 System Protection 67**

- Evidence 68
  - Properties 68
  - Measurements 70
  - What to Measure 72
  - How Many Items to Measure 73
  - Re-measurement 73

- Threats to Evidence 73
- Reporting 74
  - Report 75
  - Attestation 75
  - Threats to Reporting 76
- Trusted Computing Base Management 76
  - Number of Control Points 77
  - Threats to TCB Management 77
- Policy Engine 78
  - Difference between Engine and Policy 78
  - Policy Measurement 79
  - Fixed Policies 80
  - Default Policies 81
  - Threats to Policy 82
- Privacy Considerations 83
  - Coverage 83
  - Location Aware 84
  - Control 84
  - Opt-In 85
  - Privacy Guidelines 86
  - Threats to Privacy 86

## **Chapter 7 Physical Hardware 87**

- Randomness 88
  - Number of RNG 88
  - Threats to Randomness 89
- Persistent Storage 90
  - Threats to Persistent Storage 91
- Sequencing 91
  - Monotonic Counter 91
  - Tick Counter 92
  - Trusted Time 92
  - Sequencing Threats 93
- Inspection and Detection 94
  - Remeasurement 94
  - Inspection 95
  - Detection 95
  - The Watcher 96
  - Watchers Today and Tomorrow 99
  - Attacks on Inspection and Detection 99

Architectural Performance 100

## **Chapter 8 Between Partitions 101**

Isolation 102

Why Isolate? 103

Attacks on Isolation 103

Trusted Channel and Trusted Path 104

Why a Trusted Channel? 104

Trusted Channel Basics 106

Attacks on Trusted Channel 108

## **Chapter 9 Inside and Outside 111**

External Access 111

Cell Membrane 111

Knowledge versus Action 113

Determining the Access Points 113

Inbound Data to the Platform 114

Outbound Data to the Platform 115

Attacks on External Access 116

Protected Execution 116

Use What Is Available 118

Execution 118

## **Chapter 10 Trusted Execution Technology Objectives 119**

TXT and the Elements 119

The Basic Questions 121

What is being protected? 121

Who is the Attacker? 122

What Resources Does the Attacker Have? 122

Previous Platform Objectives 123

Ease of Use 124

Manageability 124

Privacy 125

Performance 125

Versatility 126

Backwards Compatibility 126

Protection and Attack Matrix 127

Attack Type 127

User Intent 131

Application Suitability 133

Hardware Objectives 136

- MLE Features 137
  - Protected Execution 138
  - Protected Memory Pages 138
  - Sealed Storage 138
  - Protected Input 139
  - Protected Graphics 139
  - Attestation 139

## **Chapter 11 Trusted Execution Technology Design Principles 141**

- Security Principles 142
  - Least Privilege 142
  - Economy of Mechanism 143
  - Complete Mediation 143
  - Open Design 144
  - Separation of Privilege 144
  - Least Common Mechanism 145
  - Psychological Acceptability 146
- Design Principles 146
  - High-level Requirements 146
  - Environment Requirements 147
  - User Assumptions 148
  - Attackers 148
  - Protection Requirements 149
  - Upgrade Requirements 149
  - TXT Non-requirements 150
    - MLE Measurement 150
    - Description of Measurement and Identity 150
    - Obtaining the MLE Identity 150
    - SMX Measurement Instructions 151
    - Chipset Hardware 152
    - Storing MLE Measurement in TPM 152

## **Chapter 12 Launched Environment 153**

- VMX Operation 154
- VM Control Structure 156
- VMM Launch and VM Creation 157
- Protected Virtual Machines 159
  - VMM with No Services 162
  - VMM with Kernel Features 163

- Measured Launch Environment 163
  - Measuring the MLE 164
  - Launching the MLE 165
- Protecting Secrets 166
- Establishing Secrets 168
- Boundary Conditions 169
- MLE Protection Boundary 169
  - Page Protections 170
  - Paging Mechanism 172
  - DMA Protections 173
  - TGTT 174
  - STM 175
  - MLE 175
- Other CPU Resources 176
- Keyboard and Mouse 177
- Overt Channels 177
- Boundary Summary 179
- Requirements and Boundary Comparison 180

## **Chapter 13 Attestation 181**

- TPM Design 182
- TPM Basic Components 183
  - Input and Output 183
  - Execution Engine 185
  - Program Code 185
  - Non-Volatile (NV) Storage 186
  - Volatile Storage 188
  - Secure Hash Algorithm 1 (SHA-1) 188
  - Platform Configuration Register (PCR) 191
  - Random Number Generator (RNG) 193
  - RSA Engine 193
  - Opt-in 195
  - Attestation Identity Key 196
  - Authorization 196
- TPM Functionality 197
  - Transitive Trust 197
  - Measurement Chains 198
  - Sealed Storage 202
  - Transport Session 204
- Locality 205
- Attesting To Information 207

Measurement Agent 208  
Use of the TPM 208

## **Chapter 14 Trusted Execution Technology Architecture 209**

Actual Use 211  
Measured Launched Environment 212  
Memory Arbitration 212  
Resource Assignment 213  
Communication Channel 213  
Partition Lifecycle 213  
Standard Partition 214  
Operating System 214  
Application 214  
Protection Partition 215  
Kernel 215  
Applet 216  
Application 217  
Partition Communication 217  
IPC 217  
RPC 218  
Other Mechanisms 219  
The OS, MLE, and Kernel Interaction 219  
OS, MLE, and Kernel from Same Vendor 219  
MLE and Kernel from Same Vendor 220  
OS and MLE from Same Vendor 220  
OS and Kernel from Same Vendor 221  
All Three Components from Different Vendors 221  
Application Design Options 222  
Unaware Applications 222  
Protected Component 223  
Contained Application 226  
Application Use 226

## **Chapter 15 Late Launch 229**

Launching the Protected Partition 229  
A History of SENTER 230  
Initiate the Protections at Any Time 232  
Ensure that All CPU's Participate 233  
Be Sure that the Launch Can Detect Any Tampering 234  
Knowing the Identity of the Launched Environment 235  
Ensure Properly Configured Hardware 235

- The GETSEC [SENDER] Sequence 235
  - Loading the Modules 237
  - Executing GETSEC [SENDER] 237
  - Issuing SENTER-ACK 238
  - ILP Processing 240
- SINIT Processing 242
  - SINIT Load 242
- Storing SINIT Measurement 244
  - TPM Bus Considerations 244
  - Setting the PCR 245
  - TPM Response to TPM.HASH.START 246
  - ILP Measurement Transmission 246
- Initialize ILP State 247
  - Unlocking the Chipset 247
- GETSEC [SENDER] Completion 247
- SINIT Execution 248
  - Initialize SMM Handling 248
  - Enable DMA Protection 249
  - SCLEAN Validation 249
  - MLE Loading 250
  - Passing Control to the MLE 251
- MLE Execution 251
  - Enabling Interrupts 251
  - Enabling SMI 252
- Secure Launch Recap 252
- GETSEC [SEXIT] Processing 253
  - GETSEC [SEXIT] Initiation 254
  - GETSEC [SEXIT] Validation 254
  - GETSEC [SEXIT] Rendezvous 255
  - MLE Shutdown 255
- TXT-Shutdown 256

## **Chapter 16 Configuration Concerns 257**

- TXT Chipset 257
- Memory Folding 258
  - Trusting Memory 259
  - Locking the Memory Configuration 260
  - Testing the Configuration 260
- GART/Graphics Aliasing 260
  - Ensure GART Properties 261
  - System Memory Overlap 261

- Power and Frequency 262
  - Overclocking 262
- SCHECK 263
- Additional Platform Configurations 264
- New Issues 264
- Device Support 265
  - Switch to VT-d 265
- Human Interface Design 266
- Trusted Input 267
  - Peripheral or Bus 267
  - Bus confidentiality 268
- Trusted USB Peripheral 268
  - Verification of Session Key Creation 270
- Trusted USB Controller 270
- Trusted I/O and TXT 270

## **Chapter 17 Hardware Attacks 271**

- Topologies 272
- Rogue CPU 274
  - Not Joining the Protected Environment 274
  - Not Exiting the Protected Environment 275
  - Results of Suspending the CPU 275
- RESET Protection 276
  - Reset Definition 276
  - System Memory Properties 276
  - What to Protect? 277
  - Who Determines Prior State? 277
  - Protection Sequence 278
  - Setting the ICH Flag 279
  - Adding the TPM 280
  - State Table 281
- SCLEAN AC Module 281
  - Running SCLEAN 282
  - Registering SCLEAN 284
- INIT Protection 286
- S2/S3/S4 Sleep Protection 287
- SMI Handling 288
  - SMM Transfer Module 289
  - SMM Loading 290
  - STM MLE Negotiation 292

- Bus Attacks 293
  - Front Side Bus 293
  - Hublink 294
  - Low Pin Count Bus 294

## **Chapter 18 Launch Control Policy 295**

- Policy Engine and Policies 295
  - Age Example 295
- Measurability & Reporting 297
  - Policy Engine Evidence 298
  - Policy Evidence 298
- Policy Evaluation 298
- Exceptions 299
- Launch Control Policy 299
  - Why control 300
  - Proactive Control 302
  - Who wants control 305
  - List requirements 306
- LCP Additions 310
  - Launch Environment 310
  - Additional policies 310

## **Chapter 19 Services 311**

- Typical services 312
  - Auditing 312
  - Trusted Path 314
  - Out of Band 316
- Enclave and Platform 317
  - Combining Enclaves and Platforms 318
  - Enclave Organization 320
  - How many apps in a partition 321
  - Elements for an enclave 322
- Services 322

## **Chapter 20 Defending the Platform Against Attacks 323**

- Vulnerabilities 324
- The Example Application 324
  - The Attacker's Goal 325
  - Application Functionality 325
  - Application Design 325
  - Vulnerabilities 327

- Underlying V5 Vulnerabilities 329
  - Memory Access 329
  - Driver Manipulation 330
  - Uncontrolled Program Access 330
- What Remains 331
  - Isolation 331
  - Hardware Attacks 332
- Matching Requirements 332

## **Chapter 21 The Future 335**

- How did we do 335
- New Attacks 336
  - Changing the Protection Boundary 336
  - Devious Attackers 336
  - Being Perfect 336
- New Features 337
  - Chipset Topologies 337
  - SEXIT ACM 338
  - Additional Hardware Protections 338
- Following the Principles 338