

The Intel Safer Computing Initiative

Building Blocks for Trusted Computing

David Grawrock

Intel
PRESS

Copyright © 2006 Intel Corporation. All rights reserved.

ISBN 0-9764832-6-2

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except as permitted under Sections 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4744. Requests to the Publisher for permission should be addressed to the Publisher, Intel Press, Intel Corporation, 2111 NE 25 Avenue, JF3-330, Hillsboro, OR 97124-5961. E-mail: intelpress@intel.com.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in professional services. If professional advice or other expert assistance is required, the services of a competent professional person should be sought.

Intel Corporation may have patents or pending patent applications, trademarks, copyrights, or other intellectual property rights that relate to the presented subject matter. The furnishing of documents and other materials and information does not provide any license, express or implied, by estoppel or otherwise, to any such patents, trademarks, copyrights, or other intellectual property rights.

Intel may make changes to specifications, product descriptions, and plans at any time, without notice.

Fictitious names of companies, products, people, characters, and/or data mentioned herein are not intended to represent any real individual, company, product, or event.

Intel products are not intended for use in medical, life saving, life sustaining, critical control or safety systems, or in nuclear facility applications.

Intel, Intel logo, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

† Other names and brands may be claimed as the property of others.

This book is printed on acid-free paper. ♻️

Publisher: Richard Bowles

Content Architect: Stuart Goldstein

Editor: David B. Spencer

Text Design & Composition: Wasser Studios

Graphic Art: Wasser Studios (illustrations), Ted Cyrek (cover)

Library of Congress Cataloging in Publication Data:

Printed in the United States of America

10 9 8 7 6 5 4 3 2 1

First printing, March 2006

Contents

Foreword xv

Preface xix

Part I Background Information 1

Chapter 1 Trusted Computing 3

The Basic Problem of Trust 4

The Trusted Computer and LaGrande Technology 5

Basic Definitions 6

Our Definition of Trust 6

The Trust Decision 7

The Platform 8

The Client 8

Owner, User, and Operator 9

The Weakest Link 10

Protection in the Enclave 12

Effect of Providing More Protections 12

Basic Cryptography 13

Symmetric Encryption 13

Asymmetric Encryption 13

Combination 14

Cryptographic Hash 14

| | |
|-----------------------------------|----|
| Trusted Channel and Trusted Path | 15 |
| Trusted Channel | 15 |
| Trusted Path | 15 |
| Combination | 15 |
| What is LaGrande Technology (LT)? | 16 |

Chapter 2 History of Trusted Computing 17

| | |
|--|----|
| Early Papers | 18 |
| 1970 Task Force | 18 |
| Bell-LaPadula | 20 |
| The Rainbow Series | 20 |
| Industry Response | 21 |
| The Future through the Past | 22 |
| Personal Computers | 23 |
| CPU Internals | 25 |
| Protected Mode | 25 |
| Memory Management | 26 |
| Front-side Bus | 28 |
| Multiple CPU Systems | 28 |
| MCH | 28 |
| Memory | 28 |
| Display Adapter | 28 |
| ICH | 29 |
| Keyboard | 29 |
| USB | 29 |
| LPC Bus | 29 |
| Current Intel® Architecture Security Support | 30 |
| Rings | 30 |
| Protected Mode | 30 |
| Paging | 31 |
| Security Properties | 31 |

Part II What Is Happening Today? 33

Chapter 3 The Current Environment 35

| | |
|------------------|----|
| Platform | 36 |
| Hardware | 36 |
| Operating System | 37 |
| Ring Use | 37 |
| Drivers | 38 |
| Configuration | 39 |

| | |
|----------------------------|----|
| Applications | 39 |
| Installation | 39 |
| Drivers | 39 |
| Configuration | 39 |
| Malware | 40 |
| Malware Components | 40 |
| Break Once, Run Everywhere | 41 |
| Configurations | 42 |
| Finding Bad Platforms | 42 |

Chapter 4 Anatomy of an Attack 43

| | |
|----------------------------|----|
| Programmer versus Attacker | 45 |
| Application Today | 46 |
| Application Components | 47 |
| Display Windows | 48 |
| Reading Keystrokes | 48 |
| Password Processing | 49 |
| Program Decision | 49 |
| Malware Attack Points | 50 |
| Manipulate Memory | 50 |
| Manipulate Input | 52 |
| Manipulate Output | 53 |
| Attack Overview | 55 |
| Mitigating Attacks | 56 |
| Hardware Mitigations | 56 |

Part III LaGrande Technology Design 57

Chapter 5 LaGrande Technology Objectives 59

| | |
|--|----|
| The Basic Questions | 60 |
| What is Being Protected? | 60 |
| Who is the Attacker? | 60 |
| What Resources Does the Attacker Have? | 61 |
| Previous Platform Objectives | 62 |
| Ease of Use | 63 |
| Manageability | 63 |
| Privacy | 63 |
| Performance | 64 |
| Versatility | 64 |
| Backwards Compatibility | 65 |

- Protection and Attack Matrix 66
 - Attack Type 66
 - User Intent 70
 - Application Suitability 72
- The Features 76
 - Protected Execution 76
 - Protected Memory Pages 77
 - Sealed Storage 77
 - Protected Input 77
 - Protected Graphics 78
 - Attestation 78

Chapter 6 LaGrande Technology Design Principles 79

- Security Principles 80
 - Least Privilege 80
 - Economy of Mechanism 81
 - Complete Mediation 81
 - Open Design 82
 - Separation of Privilege 82
 - Least Common Mechanism 83
 - Psychological Acceptability 83
- Design Principles 84
 - High-level Requirements 84
 - Environment Requirements 84
 - User Assumptions 85
 - Attackers 85
 - Protection Requirements 86
 - Upgrade Requirements 86
 - LT Non-requirements 86
- LT Protection Boundary 87
 - Page Protections 88
 - Paging Mechanism 90
 - NoDMA 91
 - TGTT 92
 - STM 93
 - VMM 93

| | |
|---|-----|
| VMM Measurement | 94 |
| Description of Measurement and Identity | 94 |
| Obtaining the VMM Identity | 94 |
| SMX Measurement Instructions | 95 |
| Chipset Hardware | 96 |
| Storing VMM Measurement in TPM | 96 |
| Other CPU Resources | 97 |
| Keyboard and Mouse | 98 |
| Overt Channels | 98 |
| Boundary Summary | 100 |
| Requirements and Boundary Comparison | 101 |

Chapter 7 Protected Execution 103

| | |
|----------------------------|-----|
| VMX Operation | 104 |
| VM Control Structure | 106 |
| VMM Launch and VM Creation | 107 |
| Protected Virtual Machines | 109 |
| VMM with No Services | 112 |
| VMM with Kernel Features | 112 |
| Measured VMM | 113 |
| Measuring the VMM | 114 |
| Launching the VMM | 115 |
| Protecting Secrets | 116 |
| Establishing Secrets | 117 |
| Boundary Conditions | 118 |

Chapter 8 Attestation 119

| | |
|---------------------------------------|-----|
| TPM Design | 120 |
| TPM Basic Components | 121 |
| Input and Output | 121 |
| Execution Engine | 123 |
| Program Code | 123 |
| Non-Volatile (NV) Storage | 124 |
| Volatile Storage | 126 |
| Secure Hash Algorithm 1 (SHA-1) | 126 |
| Platform Configuration Register (PCR) | 129 |
| Random Number Generator (RNG) | 131 |
| RSA Engine | 131 |
| Opt-in | 133 |
| Attestation Identity Key | 134 |
| Authorization | 134 |

- TPM Functionality 135
 - Transitive Trust 135
 - Sealed Storage 136
 - Transport Session 138
- Locality 139
- Attesting To Information 141
 - Measurement Agent 142
- Use of the TPM 142

Chapter 9 Protected Input and Output 143

- Trusted Channel and Trusted Path 144
- Why a Trusted Channel? 145
- Trusted Channel Basics 146
 - Hardware Trusted Channels 147
 - Cryptographic Trusted Channels 147
 - Trusted Channel Device Focus 149
- Device Support 149
- Secured Discrete Graphics 150
- Secured Integrated Graphics 151
 - Trusted Sprite Model 151
 - Resource Management 152
 - Panic Blue Screen 154
- Human Interface Design 155
- Trusted Input 155
 - Peripheral or Bus 156
 - Trusted Input Driver Endpoint 157
- Trusted USB Peripheral 157
 - Verification of Session Key Creation 159
- Trusted USB Controller 159
- Trusted USB Operation 160
 - Trusted USB Teardown 161
- Trusted Mobile Keyboard Controller 161
 - TMKBC Overview 163
 - TMKBC Initialization 163
 - TMKBC Operation 163
 - TMKBC Teardown 164
- Trusted I/O and LT 164

Part IV LaGrande Technology Architecture 165**Chapter 10 LaGrande Technology Architecture 167**

- Actual Use 169
- Measured Virtual Machine Monitor 170
 - Memory Arbitration 170
 - Resource Assignment 171
 - Communication Channel 171
 - Partition Lifecycle 171
- Standard Partition 172
 - Operating System 172
 - Application 172
- Protected Partition 173
 - Kernel 173
 - Applet 174
 - Application 175
- Partition Communication 175
 - IPC 176
 - RPC 176
 - Other Mechanisms 176
- The OS, MVMM, and Kernel Interaction 177
 - OS, MVMM, and Kernel from Same Vendor 177
 - MVMM and Kernel from Same Vendor 177
 - OS and MVMM from Same Vendor 178
 - OS and Kernel from Same Vendor 178
 - All Three Components from Different Vendors 179
- Application Design Options 180
 - Unaware Applications 180
 - Protected Component 181
 - Contained Application 184
- Application Use 184

Chapter 11 Late Launch 185

- Launching the Protected Partition 186
 - A History of SENTER 187
 - Initiate the Protections at Any Time 188
 - Ensure that All CPUs Participate 189
 - Be Sure that the Launch Can Detect Any Tampering 191
 - Knowing the Identity of the Launched Environment 191
 - Ensure Properly Configured Hardware 191

- The GETSEC [SENDER] Sequence 192
 - Loading the Modules 193
 - Executing GETSEC [SENDER] 194
 - Issuing SENTER-ACK 195
 - ILP Processing 196
- SINIT Processing 198
 - SINIT Load 198
- Storing SINIT Measurement 200
 - TPM Bus Considerations 200
 - Setting the PCR 200
 - TPM Response to TPM.HASH.START 201
 - ILP Measurement Transmission 202
- Initialize ILP State 202
 - Unlocking the Chipset 203
- GETSEC [SENDER] Completion 203
- SINIT Execution 203
 - Initialize SMM Handling 204
 - Enable NoDMA 205
 - SCLEAN Validation 205
 - MVMM Loading 206
 - Passing Control to the MVMM 207
- MVMM Execution 207
 - Enabling Interrupts 207
 - Enabling SMI 208
- Secure Launch Recap 208
- GETSEC [SEXIT] Processing 209
 - GETSEC [SEXIT] Initiation 210
 - GETSEC [SEXIT] Validation 211
 - GETSEC [SEXIT] Rendezvous 211
 - MVMM Shutdown 211
- LT-Shutdown 212

Chapter 12 Configuration Concerns 213

- LT Chipset 213
- Memory Folding 214
 - Trusting Memory 215
 - Locking the Memory Configuration 216
 - Testing the Configuration 216

| | |
|------------------------------------|-----|
| GART/Graphics Aliasing | 216 |
| Ensure GART Properties | 217 |
| System Memory Overlap | 218 |
| Power and Frequency | 218 |
| Overclocking | 219 |
| SCHECK | 220 |
| Additional Platform Configurations | 220 |
| New Issues | 220 |

Chapter 13 Hardware Attacks 221

| | |
|---------------------------------------|-----|
| Rogue CPU | 222 |
| Not Joining the Protected Environment | 222 |
| Not Exiting the Protected Environment | 223 |
| Results of Suspending the CPU | 223 |
| RESET Protection | 223 |
| Reset Definition | 224 |
| System Memory Properties | 224 |
| What to Protect? | 225 |
| Who Determines Prior State? | 225 |
| Protection Sequence | 226 |
| Setting the ICH Flag | 227 |
| Adding the TPM | 227 |
| State Table | 228 |
| SCLEAN AC Module | 228 |
| Running SCLEAN | 229 |
| Registering SCLEAN | 231 |
| INIT Protection | 234 |
| S2/S3/S4 Sleep Protection | 234 |
| SMI Handling | 236 |
| SMM Transfer Module | 237 |
| SMM Loading | 238 |
| STM MVMM Negotiation | 240 |
| Bus Attacks | 241 |
| Front Side Bus | 241 |
| Hublink | 241 |
| Low Pin Count Bus | 242 |

Part V The Bottom Line 243

Chapter 14 Defending the Platform Against Attacks 245

- Vulnerabilities 246
- The Example Application 246
 - The Attacker's Goal 247
 - Application Functionality 247
 - Application Design 247
 - Vulnerabilities 249
- Underlying V4 Vulnerabilities 251
 - Memory Access 251
 - Driver Manipulation 252
 - Uncontrolled Program Access 253
- What Remains 253
 - Isolation 253
 - Hardware Attacks 254
- Matching Requirements 255

Chapter 15 The Future 257

- New Attacks 257
 - Changing the Protection Boundary 258
 - Devious Attackers 258
 - Being Perfect 258
- New Features 259
 - Chipset Topologies 259
 - SEXIT ACM 260
 - Additional Hardware Protections 260
- Following the Principles 261

Glossary 263

References 269

Index 271