

Table of Contents

Acknowledgements	xv
README.IST	1
The Video Game Console Market	2
About Hackers and Hacking	4
The Politics of Hacking	6
The People Behind the Hacks	10
Voiding The Warranty	15
Tools of the Trade	15
Tools to Open Things Up	15
Tools to Attach and Remove Components	17
Tools to Test and Diagnose	18
Tools for Design	20
Deconstructing the Xbox	21
Step 1: Safety First	22
Step 2: Remove Case Screws	22
Step 3: Remove the Top Cover	25
Step 4: Move the Disk Drives	25
Step 5: Remove the Disk Drives (Optional)	27
Re-assembling the Xbox	28
Thinking Inside The Box	31
Reading a Circuit Board	32
Circuit Board Basics	32
Components	34
Test Points	39
Xbox Architecture	40
High-Level Organization	40
Functional Details	42
CPU	42
Northbridges and Southbridges	44
RAM	45
ROM	46

<i>Odds and Ends</i>	47
Pattern Matching	48
Comparison: Xbox Versus the PC	49
Contrast: Xbox Versus the Gamecube	50
Installing a Blue LED	53
What You'll Need	54
Removing The Xbox Front Panel	54
Removing the Front Panel Circuit Board	58
Installing the Blue LED	59
Re-Assembling the Front Panel	63
Debugging	65
Building a USB Adapter	67
Starting Materials	67
Strategy	69
Implementation	69
Replacing a Broken Power Supply	73
Diagnosing a Broken Power Supply	74
Replacing the Power Supply	76
Strategy	77
Procedure	78
Building the Xbox Power Cable	78
Installing the Replacement Power Supply	84
Operating with the Replacement Power Supply	85
Debugging Tips	87
The Best Xbox Game: Security Hacking	89
First Encounters with a Paranoid Design	89
To Snarf a ROM	90
An Encounter with Microsoft	92
Analyzing the ROM Contents	93
A Brief Primer on Security	101
Who Needs Security, Anyways?	101
A Brief Primer on Cryptography	104
Classes of Cryptographic Algorithms	105
SHA-1 Hash	107
TEA	109
RC-4	111
RSA	113
The Rest of the Picture	116
Reverse Engineering Xbox Security	119
Extracting Secrets From Hardware	119
Eavesdropping a High Speed Bus	122

<i>Tapping the Bus on a Budget</i>	122
<i>Building the Data Logger</i>	128
<i>Determining the Bus Order and Polarity</i>	130
Making Sense of the Captured Data	131
Sneaking In the Back Door	137
Back Doors and Security Holes	138
Visor Jam Table Attacks	139
MIST Premature Unmap Attack I	140
Microsoft Retaliates	141
Reverse Engineering v1.1 Security I	142
The Threat of Back Doors	147
More Hardware Projects	151
The LPC Interface	151
LPC Interface on the Xbox	152
Using the LPC Interface	153
The Other 64 MB of SDRAM	155
Xbox-VGA	157
Mass Storage Replacement	158
Developing Software for the Xbox	161
Xbox-Linux	161
Installing Xbox-Linux	162
“Project B”	166
OpenXDK	171
Caveat Hacker	173
Caveat Hacker: A Primer on Intellectual Property by Lee Tien	175
Classical Intellectual Property Law: An Overview	175
<i>Copyright</i>	176
The Traditional View of Reverse Engineering	180
<i>Trade Secrecy and “Improper Means”</i>	180
<i>Copyright Law and the Problem of Intermediate Copying</i>	181
<i>Patent Law</i>	182
New Challenges for Reverse Engineers	183
<i>The DMCA and the Problem of Unauthorized Access</i>	184
<i>Unauthorized Access</i>	184
<i>Circumvention Technologies</i>	185
<i>Navigating the DMCA’s Exemptions</i>	185
1201(f): reverse-engineering for interoperability	186
1201(g): encryption research	187
1201(j): security research	187
<i>End-user License Agreements and Contractual Prohibitions on</i> <i>Reverse-Engineering</i>	187
The Responsible Hacker: Ignorance is no Defense	189
Reverse Engineering as “The Freedom to Tinker” and other Legal Issues	191

Onward!	193
The Hacking Community	193
Hacking Fora	194
Making a Contribution	195
Trusted Computing	197
Taking a Step Back	199
Palladium versus TCPA	202
Hacking the Trusted PC	203
Looking Forward	205
Concluding Thoughts	206
Where to Get Your Hacking Gear	207
Vendors for Hobbyists	207
Prepared Equipment Order Forms	209
Soldering Techniques	211
Introduction to Soldering	211
Use Flux	212
Starter Tips	213
Surface Mount Soldering	214
Technique for Simple Components	215
Technique for Complex Components	216
Technique for Removing Components	219
Getting Into PCB Layout	223
Philosophy and Design Flow	223
Refining your Idea	224
Schematic Capture	224
Board Layout	226
General Placement and Routing Guidelines	227
<i>Leave Space for via Fanouts on Surface Mount Devices</i>	228
<i>Know your Special Traces</i>	229
<i>Establish Preferred Routing Directions for Each Layer</i>	231
<i>Stack a Board with Orthogonal Layers</i>	231
<i>On Two-Layer Boards, use Fingers to Bus Power</i>	231
<i>Hints on Using an Auto-router</i>	232
CAD Tools	232
Board Fabrication Companies	233
Sierra Proto Express	233
Data Circuit Systems	233
Advanced Circuits	234
Alberta Printed Circuits	234
Starter Projects	234
Getting Started with FPGAs	237
What is an FPGA?	237
Designing for an FPGA	239
Project Ideas	243

Where to Buy	244
Debugging: Hints and Tips	247
Don't Panic!	247
Understand the System	247
Observe Symptoms	248
Common Bugs	249
Recovering from a Lifted Trace or Pad	252
Xbox Hardware Reference	257
Power Supply Pinout	257
Video Connector Pinout	258
USB Connector Pinout	260
Ethernet Connector Pinout	261
ATA Connector Pinout	262
DVD-ROM Power Connector	263
LPC Connector	264
Fan Connector	265
Front Panel Connector	265
Index of Chapters	267

