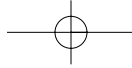


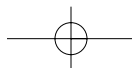
Contents

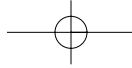
Foreword	xxvii
Introduction	xxxv
Part I Introduction to Hardware Hacking	1
Chapter 1 Tools of the Warranty Voiding Trade	3
Introduction	4
The Essential Tools	4
Taking it to the Next Level	6
Hardcore Hardware Hackers Only	8
Where to Obtain the Tools	10
Chapter 2 Electrical Engineering Basics	13
Introduction	14
Fundamentals	14
Bits, Bytes, and Nibbles	14
Reading Schematics	18
Voltage, Current, and Resistance	20
Direct Current and Alternating Current	21
Resistance	22
Ohm's Law	22
Basic Device Theory	23
Resistors	23
Capacitors	25
Diodes	28
Transistors	30
Integrated Circuits	32
Soldering Techniques	34



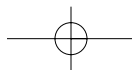
xiv Contents

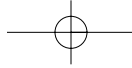
Hands-On Example: Soldering a Resistor to a Circuit Board	34
Desoldering Tips	36
Hands-On Example: SMD Removal Using ChipQuik	37
Common Engineering Mistakes	40
Web Links and Other Resources	41
General Electrical Engineering Books	41
Electrical Engineering Web Sites	42
Data Sheets and Component Information	43
Major Electronic Component and Parts Distributors	43
Obsolete and Hard-to-Find Component Distributors	43
Part II Hardware Hacks	45
Chapter 3 Declawing Your CueCat	47
Introduction	48
Model Variations	49
Opening the CueCat	51
Preparing for the Hack	51
Opening the Four-Screw PS/2 CueCat	51
Opening the Two-Screw PS/2 CueCat	54
Opening the USB CueCat	55
Removing the Unique Identifier	56
Preparing for the Hack	57
Removing the UID: Four-Screw PS/2CueCat	57
Removing the UID: Two-Screw PS/2CueCat	60
Removing the UID: USB CueCat	62
Under the Hood: How the Hack Works	64
Removing the Proprietary Barcode Encoding	68
Preparing for the Hack	68
Removing the Encoding from the Four-Screw PS/2 CueCat	69
Removing the Encoding from the Two-Screw PS/2 CueCat	71
Removing the Encoding from the USB CueCat	73
Under the Hood: How the Hack Works	74



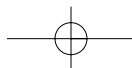


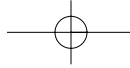
Technical Information	76
The CueCat Encoding Scheme	76
More Physical Model Variations	78
More History of Political and Legal Issues	80
CueCat Litter Box: Web Links and Other Resources	82
Open-Source CueCat Software and Drivers	83
DigitalConvergence Patents for CueCat Technologies	83
Chapter 4 Case Modification: Building a Custom Terabyte FireWire Hard Drive	83
Introduction	84
Case Mod Primer	84
Creating a 1.2TB FireWire RAID	85
Preparing for the Hack	85
Performing the Hack	86
Under the Hood: How the Hack Works	92
Custom Case Modification for the FireWire RAID	94
Preparing for the Hack	94
Performing the Hack	95
Under the Hood: How the Hack Works	105
Additional Resources	108
Case Modifications	109
Chapter 5 Macintosh	111
Compubrick SE	112
Preparing for the Hack	113
Performing the Hack	114
Taking Apart the Mac	114
Encasing the Speaker	120
Covering the Mouse and the Keyboard	121
Encasing the Disk Drive	123
Encasing the Hard Drive	125
Encasing the Motherboard	127
Encasing the CRT	129
How the Hack Works	131
Building a UFO Mouse	132



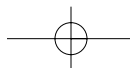
**xvi** Contents

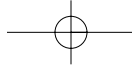
Preparing for the Hack	133
Performing the Hack	134
Opening the Mouse	134
Drilling the Hole	136
Soldering the LED	137
Reassembling the Mouse	138
How the Hack Works	140
Adding Colored Skins to the Power Macintosh G4 Cube	140
Preparing for the Hack	141
Performing the Hack	142
Under the Hood: How the Hack Works	145
Other Hacks and Resources	145
Desktop Hacks	145
Laptop Hacks	146
Electrical and Optical Hacks	146
Case Mods	146
Software	147
Discussion	147
Chapter 6 Home Theater PCs	149
Introduction	150
Before You Begin: Research and Plan	151
How Much Could It Cost?	152
Did Someone Already Build It?	153
The Components of an HTPC Project	154
The Display	155
What Are Your Options for Higher-Quality Video Display?	157
The Video Card	160
The Case	160
The Hard Drives	161
Speed Considerations	163
Sshhhh... Quiet Operations	164
Optical Drives	164
The CPU	165
The Sound Card	166



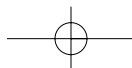


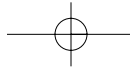
	Contents	xvii
The Controller	167	
The Software	167	
Building a Windows HTPC	171	
Preparing for the Hack	171	
Performing the Hack: Software	175	
Eazylook	177	
Using the Launcher	178	
Using Guide Plus+	178	
CDex	180	
FairUse	180	
Windows Summary	185	
Building a Linux HTPC	185	
Preparing for the Hack	185	
Performing the Hack: Hardware	185	
Performing the Hack: Software	192	
Installing the Video Capture Drivers	192	
Install MPlayer and CODECs	194	
Installing MythTV	194	
Linux Summary	197	
Further Hacking and Advanced Topics	198	
Chapter 7 Hack Your Atari 2600 and 7800	199	
Introduction	200	
The Atari 7800 ProSystem	201	
Hacks in This Chapter	202	
Atari 2600 Left-Handed Joystick Modification	202	
Preparing for the Hack	203	
Performing the Hack	204	
Use an NES Control Pad with Your 2600	207	
Preparing for the Hack	207	
Performing the Hack	209	
Atari 2600 Stereo Audio Output	214	
Preparing for the Hack	216	
Performing the Hack	216	
Under the Hood: How the Hack Works	223	
Atari 7800 Blue LED Modification	223	



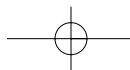

xviii Contents

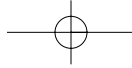
Preparing for the Hack	223
Performing the Hack	224
Under the Hood: How the Hack Works	227
Atari 7800 Game Compatibility Hack to Play Certain	
2600 Games	228
Preparing for the Hack	229
Performing the Hack	230
Under the Hood: How the Hack Works	232
Atari 7800 Voltage Regulator Replacement	232
Preparing for the Hack	233
Performing the Hack	233
Under the Hood: How the Hack Works	236
Atari 7800 Power Supply Plug Retrofit	237
Preparing for the Hack	238
Performing the Hack	239
Other Hacks	242
2600 Composite/S-Video Modifications	242
Atari 7800 Composite and S-Video Output	243
Sega Genesis to Atari 7800 Controller Modification	243
NES Control Pad to Atari 7800 Controller Modification	243
Atari 7800 DevOS Modification and Cable Creation	243
Atari Resources on the Web	244
Chapter 8 Hack Your Atari 5200 and 8-Bit Computer	247
Introduction	248
The Atari 5200 SuperSystem	249
Hacks in This Chapter	250
Atari 5200 Blue LED Modification	250
Preparing for the Hack	251
Performing the Hack	251
Under the Hood: How the Hack Works	256
Creating an Atari 5200 Paddle	256
Preparing for the Hack	257
Performing the Hack: Disassembling the Paddle	
Controller	258



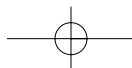


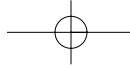
Performing the Hack: Building the 5200 Paddle Controller	260
Performing the (Optional) Hack: Weighted Dial	266
Under the Hood: How the Hack Works	267
Free Yourself from the 5200 Four-Port Switchbox	268
Preparing for the Hack	269
Performing the Hack	271
Under the Hood: How the Hack Works	279
Build Atari 8-Bit S-Video and Composite Cables	280
Preparing for the Hack	281
Performing the Hack	282
Cable Hack Alternatives	288
Under the Hood: How the Hack Works	289
Technical Information	289
Other Hacks	290
Atari 5200 Four-Port VCS Cartridge Adapter Fix	290
Atari 5200 Composite/S-Video Modification	290
Atari 8-Bit SIO2PC Cable	291
Atari Resources on the Web	291
Chapter 9 Hacking the PlayStation 2	293
Introduction	294
Commercial Hardware Hacking: Modchips	294
Getting Inside the PS2	296
Mainboard Revisions	296
Identifying Your Mainboard	297
Opening the PS2	298
Installing a Serial Port	302
Preparing for the Hack	303
Performing the Hack	304
Testing	309
Under the Hood: How the Hack Works	310
Booting Code from the Memory Card	310
Preparing for the Hack	310
Performing the Hack: Preparing Title.DB	311
Choosing BOOT.ELF	313



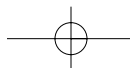
**xx** Contents

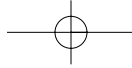
Saving TITLE.DB to the Memory Card	314
Independence!	314
Under the Hood: How the Hack Works	314
Other Hacks: Independent Hard Drives	316
PS2 System Overview	316
Understanding the Emotion Engine	317
The Serial I/O Port	318
The I/O Processor	321
The Sub-CPU Interface	321
Additional Web Resources	321
Chapter 10 Wireless 802.11 Hacks	323
Introduction	324
Wireless NIC/PCMCIA Card Modifications:	
Adding an External Antenna Connector	325
Preparing for the Hack	326
Performing the Hack	327
Removing the Cover	327
Moving the Capacitor	329
Attaching the New Connector	331
Under the Hood: How the Hack Works	332
OpenAP (Instant802): Reprogramming Your Access Point	
with Linux	332
Preparing for the Hack	333
Performing the Hack	334
Installing the SRAM Card	335
Power Me Up, Scotty!	338
Under the Hood: How the Hack Works	338
Having Fun with the Dell 1184 Access Point	338
Preparing for the Hack	339
Performing the Hack	340
Under the Hood: How the Hack Works	345
Summary	345
Additional Resources and Other Hacks	345
User Groups	345
Research and Articles	346



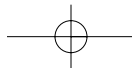


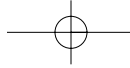
Products and Tools	346
Chapter 11 Hacking the iPod	349
Introduction	350
Opening Your iPod	353
Preparing for the Hack	354
First Generation iPods	355
Second and Third-Generation iPods	356
Replacing the iPod Battery	359
Preparing for the Hack	360
Battery Replacement: First- and Second-Generation iPods	361
Battery Replacement: Third-Generation iPods	365
Upgrading a 5GB iPod's Hard Drive	371
Preparing for the Hack	372
Performing the Hack	372
From Mac to Windows and Back Again	381
Preparing for the Hack	381
Going from Windows to Macintosh	381
Going from Macintosh to Windows	383
iPod Diagnostic Mode	384
The Diagnostic Menu	384
Disk Check	387
Additional iPod Hacks	388
Installing Linux on an iPod	388
Repairing the FireWire Port	388
Scroll Wheel Fix	389
iPod Resources on the Web	390
Chapter 12 Can You Hear Me Now? Nokia 6210 Mobile Phone Modifications	391
Introduction	392
Nokia 6210 LED Modification	393
Preparing for the Hack	393
Performing the Hack	395
Opening the Nokia 6210	395
Removing the Old LEDs	400



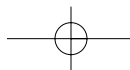
**xxii** Contents

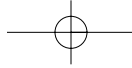
Inserting the New LEDs	401
Increasing the LED Power	402
Putting the Phone Back Together	403
Under the Hood: How the Hack Works	404
Data Cabling Hacks	406
Data Cables	407
Flashing Cables	410
Net Monitor	411
Other Hacks and Resources	415
Chapter 13 Upgrading Memory on Palm Devices	417
Introduction	418
Model Variations	419
Hacking the Pilot 1000 and Pilot 5000	420
Preparing for the Hack	420
Removing the Memory Card	422
Adding New Memory	423
Under the Hood: How the Hack Works	427
Hacking the PalmPilot Professional and PalmPilot Personal	429
Preparing for the Hack	429
Removing the Memory Card	429
Adding New Memory	430
Under the Hood: How the Hack Works	433
Hacking the Palm m505	436
Preparing for the Hack	436
Opening the Palm	437
Removing the Main Circuit Board	439
Removing the Memory	441
Adding New Memory	442
Under the Hood: How the Hack Works	445
Technical Information	447
Hardware	447
File System	448
Memory Map	448



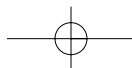


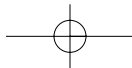
	Contents	xxiii
Database Structure	449	
Palm Links on the Web	450	
Technical Information	450	
Palm Hacks	450	
More Memory Upgrades	450	
Part III Hardware Hacking Technical Reference	451	
Chapter 14 Operating Systems Overview	453	
Introduction	454	
OS Basics	454	
Memory	455	
Physical Memory	455	
Virtual Memory	457	
File Systems	458	
Cache	459	
Input/Output	460	
Processes	460	
System Calls	461	
Shells, User Interfaces, and GUIs	461	
Device Drivers	462	
Block and Character Devices	464	
Properties of Embedded Operating Systems	466	
Linux	467	
Open Source	467	
History	468	
Embedded Linux (uClinux)	469	
Product Examples: Linux on Embedded Systems	470	
VxWorks	470	
Product Examples: VxWorks on Embedded Systems	470	
Windows CE	471	
Concepts	471	
Product Examples: Windows CE on Embedded Systems	472	
Summary	473	
Additional References and Further Reading	473	





Chapter 15 Coding 101	475
Introduction	476
Programming Concepts	476
Assignment	477
Control Structures	478
Looping	479
Conditional Branching	480
Unconditional Branching	481
Storage Structures	482
Structures	483
Arrays	484
Hash Tables	485
Linked Lists	486
Readability	488
Comments	488
Function and Variable Names	488
Code Readability: Pretty Printing	489
Introduction to C	490
History and Basics of C	490
Printing to the Screen	490
Data Types in C	493
Mathematical Functions	493
Control Structures	496
<i>For</i> Loops	496
<i>While</i> Loops	496
<i>If/Else</i>	498
<i>Switch</i>	500
Storage Structures	501
Arrays, Pointers, and Character Strings	501
Structures	506
Function Calls and Variable Passing	507
System Calls and Hardware Access	508
Summary	509
Debugging	509
Debugging Tools	509





	Contents	xxv
The <i>printf</i> Method	510	
Introduction to Assembly Language	512	
Components of an Assembly Language Statement	513	
Labels	513	
Operations	515	
Operands	515	
Sample Program	516	
Summary	518	
Additional Reading	518	
Index	519	

