Contents

Introduction 9

0 A CFP with POC 13
0:1 Let us begin! 13
0:2 iPod Antiforensics
    by Travis Goodspeed 15
0:3 ELF's are dorky, Elves are cool
    by S. Bratus and J. Bangert 20
0:4 Epistle to Hats of All Colors
    by Manul Laphroaig 29
0:5 Returning from ELF to Libc
    by Rebecca .Bx Shapiro 32
0:6 GTFO or #FAIL
    by FX of Phenoelit 35

1 Proceedings of the Society of PoC∥GTFO 37
1:1 Lend me your ears! 37
1:2 RNG in four lines of Javascript
    by Dan Kaminsky 39
1:3 Serena Butler's TV Typewriter
    by Travis Goodspeed 47
1:4 Making a Multi-Windows PE
    by Ange Albertini 58
1:5 This ZIP is also a PDF
    by Julia Wolf 62
## Contents

1:6 Burning a Phone  
by Josh Thomas  ........................................... 65

1:7 Sermon on the Divinity of Languages  
by Manul Laphroaig  ........................................... 69

2 The Children’s Bible Coloring Book of PoC GTFO  73  
2:1 Ring them Bells!  ........................................... 73  
2:2 Build your own birdfeeder.  
by Manul Laphroaig  ........................................... 76  
2:3 A PGP Matryoshka Doll  
by Myron Aub  ........................................... 80  
2:4 Code Execution on a Tamagotchi  
by Natalie Silvanovich  ........................................... 83  
2:5 Shellcode for MSP430  
by Travis Goodspeed  ........................................... 88  
2:6 Calling putchar() from ELF  
by Rebecca .Bx Shapiro  ........................................... 96  
2:7 POKE of Death for the TRS 80/M100  
by Dave Weinstein  ........................................... 106  
2:8 This OS is also a PDF  
by Ange Albertini  ........................................... 109  
2:9 A Vulnerability in Reduced Dakarand  
by Joernchen  ........................................... 115  
2:10 Juggernauty  
by Ben Nagy  ........................................... 125

3 Address on the Smashing of Idols to Bits and Bytes  129  
3:1 Fear Not!  ........................................... 129  
3:2 Greybeard’s Luck  
by Manul Laphroaig  ........................................... 133  
3:3 This PDF is a JPEG.  
by Ange Albertini  ........................................... 140
Contents

3:4  Netwatch for SMM
    by Wise and Potter ........................................ 143

3:5  Packet-in-Packet Mitigation Bypass
    by Travis Goodspeed ....................................... 150

3:6  An RDRAND Backdoor in Bochs
    by Taylor Hornby ........................................... 159

3:7  Kosher Firmware for the Nokia 2720
    by Assaf Nativ .............................................. 166

3:8  Tetranglix Boot Sector
    by Haverinen, Shepherd, and Sethi ....................... 182

3:9  Defusing the Qualcomm Dragon
    by Josh Thomas .............................................. 187

3:10 Tales of Python’s Encoding
    by Frederik Braun .......................................... 191

3:11 Angecryption
    by Albertini and Aumasson ................................ 195

4  Tract de la Société Secrète 203

4:1  Let me tell you a story.
    by Manul Laphroaig ......................................... 203

4:2  Epistle on the Bountiful Seeds of 0Day
    by Shikhin Sethi ............................................. 206

4:3  This OS is a Boot Sector
    by Shikhin Sethi ............................................. 208

4:4  Prince of PoC
    by Peter Ferrie .............................................. 221

4:5  New Facedancer Framework
    by Gil ........................................................... 230

4:6  Power Glitching Tamagotchi
    by Natalie Silvanovich ..................................... 238

4:7  A Plausibly Deniable Cryptosystem
    by Evan Sultanik ............................................. 245
## Contents

### 4:8 Hardening Pin Tumbler Locks
by Deviant Ollam ........................................... 256

### 4:9 Intro to Chip Decapsulation
by Travis Goodspeed ......................................... 265

### 4:10 Forget Not the Humble Timing Attack
by Colin O’Flynn ............................................. 277

### 4:11 This Truecrypt is a PDF
by Ange Albertini ........................................... 286

### 4:12 How to Manually Attach a File to a PDF
by Albertini .................................................. 290

### 4:13 Ode to ECB
by Ben Nagy .................................................. 294

### 5 Address to the Inhabitants of Earth 297

#### 5:1 It started like this. ..................................... 297

#### 5:2 A Sermon on Hacker Privilege.
by Manul Laphroaig ........................................... 301

#### 5:3 ECB: Electronic Coloring Book
by Philippe Teuwen .......................................... 306

#### 5:4 An Easter Egg in PCI Express
by Jacob Torrey ............................................... 315

#### 5:5 A Flash PDF Polyglot
by Alex Inführ ............................................... 322

#### 5:6 This Multiprocessing OS is a Boot Sector
by Shikhin Sethi .............................................. 326

#### 5:7 A Breakout Board for Mini-PCIe
by Joe FitzPatrick ............................................ 338

#### 5:8 Prototyping a generic x86 backdoor in Bochs
by Matilda .................................................... 346

#### 5:9 Your Cisco blade is booting PoC||GTFO.
by Mik .......................................................... 360
5:10 I am my own NOP Sled.
   by Brainsmoke .......................... 370
5:11 Abusing JSONP with Rosetta Flash
   by Michele Spagnuolo ................... 375
5:12 Sexy collision PoCs
   by A. Albertini and M. Eichlseder .... 386
5:13 Ancestral Voices
   by Ben Nagy .............................. 398

6 Old Timey Exploitation 401
6:1 Communion with the Weird Machines .... 401
6:2 On Giving Thanks
   by Manul Laphroaig ...................... 404
6:3 Gekko the Dolphin
   by Fiora ................................. 410
6:4 This TAR archive is a PDF!
   by Ange Albertini ...................... 430
6:5 x86 Alchemy and Smuggling
   by Micah Elizabeth Scott .............. 434
6:6 Detecting MIPS Emulation
   by Craig Heffner ........................ 450
6:7 More Cryptographic Coloring Books
   by Philippe Teuwen ...................... 458
6:8 PCB Reverse Engineering
   by Joe Grand ............................. 471
6:9 Davinci Seal
   by Ryan O’Neill .......................... 480
6:10 Observable Metrics
   by Don A. Bailey ........................ 495
Contents

7 PoC GTFO, Calisthenics and Orthodontia 511
7:1 With what shall we commune this evening? . . . . 511
7:2 The Magic Number: 0xAA55
by Morgan Reece . . . . . . . . . . . . . . . . . . . 514
7:3 Coastermelt
by Micah Elizabeth Scott . . . . . . . . . . . . . . 516
7:4 The Lysenko Sermon
by Manul Laphroaig . . . . . . . . . . . . . . . . . . 525
7:5 When Scapy is too high-level
by Eric Davisson . . . . . . . . . . . . . . . . . . . 532
7:6 Abusing file formats
by Ange Albertini . . . . . . . . . . . . . . . . . . . 541
7:7 AES-NI Backdoors
by BSDaemon and Pirata . . . . . . . . . . . . . . 585
7:8 Innovations with Linux core files.
by Ryan O’Neill . . . . . . . . . . . . . . . . . . . 598
7:9 Bambaataa speaks from the past.
by Count Bambaata . . . . . . . . . . . . . . . . . . 612
7:11 Cyber Criminal’s Song
by Ben Nagy . . . . . . . . . . . . . . . . . . . . . . 620

8 Exploits Sit Lonely on the Shelf 623
8:1 Please stand; now, please be seated. . . . . . . . 623
8:2 Witches, Warlocks, and Wassenaar
by Manul Laphroaig . . . . . . . . . . . . . . . . . . 626
8:3 Compiler Bug Backdoors
by Bauer, Cuq, and Regehr . . . . . . . . . . . . . . 631
8:4 A Protocol for Leibowitz
by Goodspeed and Muur . . . . . . . . . . . . . . . 639
8:5 Jiggling into a New Attack Vector
by Mickey Shkatov . . . . . . . . . . . . . . . . . . . 659
Contents

8:6 Hypervisor Exploit, Five Years Old
by DJC and Bittman ............... 667

8:7 Stegosploit
by Saumil Shah .................... 673

8:8 On Error Resume Next
by Jeffball .......................... 714

8:9 Unbrick My Part
by Tommy Brixton ................... 718

8:10 Backdoors up my Sleeve
by JP Aumasson ...................... 720

8:11 Naughty Signals
by Russell Handorf .................. 731

8:12 Weird Crypto
by Philippe Teuwen .................. 740

Useful Tables 750

Index 773

Colophon 788