

At a Glance

Foreword xv

Part I Hacking 802.11 Wireless Technology

1	Introduction to 802.11 Hacking	3
2	Scanning and Enumerating 802.11 Networks	31
3	Attacking 802.11 Wireless Networks	63
4	Attacking WPA-Protected 802.11 Networks	89
5	Attacking 802.11 Wireless Clients	127
6	Taking It All the Way: Bridging the Air-Gap from Windows 8 ...	155

Part II Bluetooth

7	Bluetooth Classic Scanning and Reconnaissance	191
8	Bluetooth Low Energy Scanning and Reconnaissance	229
9	Bluetooth Eavesdropping	249
10	Attacking and Exploiting Bluetooth	287

Part III More Ubiquitous Wireless

11	Software-Defined Radios	327
----	-------------------------------	-----

12	Hacking Cellular Networks	359
13	Hacking ZigBee	405
14	Hacking Z-Wave Smart Homes	461
	Index	499

At a Glance

Hacking 802.11 Wireless Technology

1	Introduction to 802.11 Hacking	3
2	Scanning and Enumerating 802.11 Networks	31
3	Attacking 802.11 Wireless Networks	63
4	Attacking WPA-Protected 802.11 Networks	89
5	Attacking 802.11 Wireless Clients	127
6	Taking It All the Way: Bridging the Air-Gap from Windows 8	155

Bluetooth

7	Bluetooth Classic Scanning and Reconnaissance	191
8	Bluetooth Low Energy Scanning and Reconnaissance	229
9	Bluetooth Eavesdropping	249
10	Attacking and Exploiting Bluetooth	287

More Upstream Wireless

11	Software-Defined Radios	327
----	-------------------------------	-----

Contents

Foreword	xv
Acknowledgments	xvii
Introduction	xix

Part I Hacking 802.11 Wireless Technology

CASE STUDY: Twelve Volt Hero	2
1 Introduction to 802.11 Hacking	3
802.11 in a Nutshell	4
The Basics	4
Addressing in 802.11 Packets	5
802.11 Security Primer	5
Discovery Basics	9
Hardware and Drivers	16
A Note on the Linux Kernel	16
Chipsets and Linux Drivers	17
Modern Chipsets and Drivers	18
Cards	20
Antennas	25
Cellular Data Cards	28
GPS	28
Summary	30
2 Scanning and Enumerating 802.11 Networks	31
Choosing an Operating System	32
Windows	32
OS X	32
Linux	32
Windows Discovery Tools	33
Vistumbler	33

Windows Sniffing/Injection Tools	36
NDIS 6.0 Monitor Mode Support (NetMon/MessageAnalyzer)	36
AirPcap	38
CommView for WiFi	40
OS X Discovery Tools	44
KisMAC	44
Linux Discovery Tools	48
airodump-ng	48
Kismet	53
Advanced Visualization Techniques (PPI)	56
Visualizing PPI-Tagged Kismet Data	57
PPI-Based Triangulation (Servo-Bot)	59
Summary	62
3 Attacking 802.11 Wireless Networks	63
Basic Types of Attacks	64
Security Through Obscurity	64
Defeating WEP	71
WEP Key Recovery Attacks	71
Putting It All Together with Wifite	83
Installing Wifite on a WiFi Pineapple	83
Summary	87
4 Attacking WPA-Protected 802.11 Networks	89
Obtaining the Four-Way Handshake	91
Cracking with Cryptographic Acceleration	95
Breaking Authentication: WPA Enterprise	109
Obtaining the EAP Handshake	110
EAP-MD5	111
EAP-GTC	113
LEAP	114
EAP-FAST	115
EAP-TLS	117
PEAP and EAP-TTLS	118
Running a Malicious RADIUS Server	120
Summary	126
5 Attacking 802.11 Wireless Clients	127
browser_autopwn: A Poor Man's Exploit Server	128
Using Metasploit browser_autopwn	129
Getting Started with I-love-my-neighbors	132
Creating the AP	133
Assigning an IP Address	134
Setting Up the Routes	134
Redirecting HTTP Traffic	135
Serving HTTP Content with Squid	136

Attacking Clients While Attached to an AP	136
Associating to the Network	137
ARP Spoofing	142
Direct Client Injection Techniques	152
Summary	154
6 Taking It All the Way: Bridging the Air-Gap from Windows 8	155
Preparing for the Attack	157
Exploiting Hotspot Environments	161
Controlling the Client	163
Local Wireless Reconnaissance	164
Remote Wireless Reconnaissance	171
Windows Monitor Mode	173
Microsoft NetMon	173
Target Wireless Network Attack	180
Summary	187

Part II Bluetooth

CASE STUDY: You Can Still Hack What You Can't See	190
7 Bluetooth Classic Scanning and Reconnaissance	191
Bluetooth Classic Technical Overview	192
Device Discovery	193
Protocol Overview	193
Bluetooth Profiles	196
Encryption and Authentication	196
Preparing for an Attack	197
Selecting a Bluetooth Classic Attack Device	197
Reconnaissance	199
Active Device Discovery	200
Passive Device Discovery	210
Hybrid Discovery	211
Passive Traffic Analysis	214
Service Enumeration	221
Summary	227
8 Bluetooth Low Energy Scanning and Reconnaissance	229
Bluetooth Low Energy Technical Overview	230
Physical Layer Behavior	231
Operating Modes and Connection Establishment	231
Frame Configuration	232
Bluetooth Profiles	235
Bluetooth Low Energy Security Controls	235

- Scanning and Reconnaissance 237
- Summary 247
- 9 Bluetooth Eavesdropping** 249
 - Bluetooth Classic Eavesdropping 250
 - Open Source Bluetooth Classic Sniffing 251
 - Commercial Bluetooth Classic Sniffing 255
 - Bluetooth Low Energy Eavesdropping 265
 - Bluetooth Low Energy Connection Following 267
 - Bluetooth Low Energy Promiscuous Mode Following 274
- Exploiting Bluetooth Networks Through Eavesdropping Attacks 276
- Summary 285
- 10 Attacking and Exploiting Bluetooth** 287
 - Bluetooth PIN Attacks 288
 - Bluetooth Classic PIN Attacks 289
 - Bluetooth Low Energy PIN Attacks 294
 - Practical Pairing Cracking 297
 - Device Identity Manipulation 300
 - Bluetooth Service and Device Class 300
 - Abusing Bluetooth Profiles 304
 - Testing Connection Access 304
 - Unauthorized PAN Access 306
 - File Transfer Attacks 310
 - Attacking Apple iBeacon 314
 - iBeacon Deployment Example 315
 - Summary 323

Part III More Ubiquitous Wireless

- CASE STUDY: Failure Is Not an Option 326
- 11 Software-Defined Radios** 327
 - SDR Architecture 328
 - Choosing a Software Defined Radio 330
 - RTL-SDR: Entry-Level Software-Defined Radio 331
 - HackRF: Versatile Software-Defined Radio 332
 - Getting Started with SDRs 333
 - Setting Up Shop on Windows 333
 - Setting Up Shop on Linux 333
 - SDR# and gqrx: Scanning the Radio Spectrum 335
 - Digital Signal Processing Crash Course 342
 - Rudimentary Communication 343
 - Rudimentary (Wireless) Communication 343
 - POCSAG 344

Information as Sound	345
Picking Your Target	346
Finding and Capturing an RF Transmission	347
Blind Attempts at Replay Attacks	348
So What?	356
Summary	357
12 Hacking Cellular Networks	359
Fundamentals of Cellular Communication	360
Cellular Network RF Frequencies	360
Standards	361
2G Network Security	362
GSM Network Model	363
GSM Authentication	363
GSM Encryption	365
GSM Attacks	365
GSM Eavesdropping	366
GSM A5/1 Key Recovery	374
GSM IMSI Catcher	383
Femtocell Attacks	387
4G/LTE Security	396
LTE Network Model	397
LTE Authentication	398
LTE Encryption	400
Null Algorithm	401
Encryption Algorithms	401
Platform Security	401
Summary	403
13 Hacking ZigBee	405
ZigBee Introduction	406
ZigBee's Place as a Wireless Standard	407
ZigBee Deployments	407
ZigBee History and Evolution	408
ZigBee Layers	409
ZigBee Profiles	413
ZigBee Security	413
Rules in the Design of ZigBee Security	414
ZigBee Encryption	414
ZigBee Authenticity	415
ZigBee Authentication	416
ZigBee Attacks	417
Introduction to KillerBee	417
Network Discovery	426
Eavesdropping Attacks	427

346	Replay Attacks	436
346	Encryption Attacks	439
347	Packet Forging Attacks	441
348	Attack Walkthrough	451
350	Network Discovery and Location	451
352	Analyzing the ZigBee Hardware	453
352	RAM Data Analysis	456
352	Summary	458
14	Hacking Z-Wave Smart Homes	461
361	Z-Wave Introduction	462
362	Z-Wave Layers	462
363	Z-Wave Security	470
363	Z-Wave Attacks	474
365	Eavesdropping Attacks	474
365	Z-Wave Injection Attacks	491
366	Summary	497
374	Index	499
387	Femtocell Attacks	403
388	4G/LTE Security	404
387	Testing Connection Access	406
388	Unauthorized PAN Access	406
400	File Transfer Attacks	416
401	Attacking Apple iBeacon	416
401	iBeacon Deployment Example	416
401	Summary	423
403	Summary	423
405	13 Hacking ZigBee	427
406	ZigBee Introduction	427
407	ZigBee's Place as a Wireless Standard and Not an Ad Hoc Network	427
407	ZigBee Deployments	427
408	ZigBee History and Evolution	428
409	ZigBee Layers	428
413	ZigBee Profiles	430
413	ZigBee Security	433
414	Rules in the Design of ZigBee Security	433
414	ZigBee Encryption	433
415	ZigBee Authentication	433
416	ZigBee Authentication	433
417	ZigBee Attacks	433
417	Introduction to KillerBee	433
426	Network Discovery	433
427	Eavesdropping Attacks	433
427	Summary	433