

CONTENTS IN DETAIL

FOREWORD by Chris Evans	xvii
--------------------------------	-------------

ACKNOWLEDGMENTS	xix
------------------------	------------

INTRODUCTION	xxi
---------------------	------------

Why Car Hacking Is Good for All of Us	xxii
What's in This Book	xxiii

1 UNDERSTANDING THREAT MODELS 1

Finding Attack Surfaces	2
Threat Modeling	2
Level 0: Bird's-Eye View	3
Level 1: Receivers	3
Level 2: Receiver Breakdown	5
Threat Identification	6
Level 0: Bird's-Eye View	6
Level 1: Receivers	7
Level 2: Receiver Breakdown	10
Threat Rating Systems	11
The DREAD Rating System	11
CVSS: An Alternative to DREAD	13
Working with Threat Model Results	13
Summary	14

2 BUS PROTOCOLS 15

The CAN Bus	16
The OBD-II Connector	17
Finding CAN Connections	17
CAN Bus Packet Layout	18
The ISO-TP Protocol	19
The CANopen Protocol	20
The GMLAN Bus	20
The SAE J1850 Protocol	20
The PWM Protocol	21
The VPW Protocol	22
The Keyword Protocol and ISO 9141-2	22
The Local Interconnect Network Protocol	24
The MOST Protocol	24
MOST Network Layers	25
MOST Control Blocks	25
Hacking MOST	26

The FlexRay Bus	27
Hardware	27
Network Topology	27
Implementation	27
FlexRay Cycles	28
Packet Layout	29
Sniffing a FlexRay Network	30
Automotive Ethernet	30
OBD-II Connector Pinout Maps	31
The OBD-III Standard	33
Summary	34

3

VEHICLE COMMUNICATION WITH SOCKETCAN 35

Setting Up can-utils to Connect to CAN Devices	36
Installing can-utils	37
Configuring Built-In Chipsets	37
Configuring Serial CAN Devices	39
Setting Up a Virtual CAN Network	40
The CAN Utilities Suite	41
Installing Additional Kernel Modules	42
The can-isotp.ko Module	43
Coding SocketCAN Applications	44
Connecting to the CAN Socket	44
Setting Up the CAN Frame	45
The Procs Interface	45
The Socketcand Daemon	46
Kayak	46
Summary	49

4

DIAGNOSTICS AND LOGGING 51

Diagnostic Trouble Codes	52
DTC Format	52
Reading DTCs with Scan Tools	54
Erasing DTCs	54
Unified Diagnostic Services	54
Sending Data with ISO-TP and CAN	55
Understanding Modes and PIDs	57
Brute-Forcing Diagnostic Modes	58
Keeping a Vehicle in a Diagnostic State	60
Event Data Recorder Logging	61
Reading Data from the EDR	62
The SAE J1698 Standard	63
Other Data Retrieval Practices	63
Automated Crash Notification Systems	64
Malicious Intent	64
Summary	65

5 REVERSE ENGINEERING THE CAN BUS 67

Locating the CAN Bus	67
Reversing CAN Bus Communications with can-utils and Wireshark	68
Using Wireshark	69
Using candump	70
Grouping Streamed Data from the CAN Bus	70
Using Record and Playback	73
Creative Packet Analysis	76
Getting the Tachometer Reading	79
Creating Background Noise with the Instrument Cluster Simulator	81
Setting Up the ICSim	81
Reading CAN Bus Traffic on the ICSim	83
Changing the Difficulty of ICSim	84
Reversing the CAN Bus with OpenXC	84
Translating CAN Bus Messages	85
Writing to the CAN Bus	86
Hacking OpenXC	87
Fuzzing the CAN Bus	88
Troubleshooting When Things Go Wrong	89
Summary	90

6 ECU HACKING 91

Front Door Attacks	92
J2534: The Standardized Vehicle Communication API	92
Using J2534 Tools	93
KWP2000 and Other Earlier Protocols	94
Capitalizing on Front Door Approaches: Seed-Key Algorithms	94
Backdoor Attacks	95
Exploits	95
Reversing Automotive Firmware	96
Self-Diagnostic System	96
Library Procedures	97
Comparing Bytes to Identify Parameters	101
Identifying ROM Data with WinOLS	103
Code Analysis	106
A Plain Disassembler at Work	107
Interactive Disassemblers	110
Summary	113

7 BUILDING AND USING ECU TEST BENCHES 115

The Basic ECU Test Bench	116
Finding an ECU	116
Dissecting the ECU Wiring	117
Wiring Things Up	119

Building a More Advanced Test Bench	119
Simulating Sensor Signals	120
Hall Effect Sensors	121
Simulating Vehicle Speed	123
Summary	126

8 ATTACKING ECUS AND OTHER EMBEDDED SYSTEMS 127

Analyzing Circuit Boards	128
Identifying Model Numbers	128
Dissecting and Identifying a Chip	128
Debugging Hardware with JTAG and Serial Wire Debug	130
JTAG	130
Serial Wire Debug	132
The Advanced User Debugger	133
Nexus	134
Side-Channel Analysis with the ChipWhisperer	134
Installing the Software	135
Prepping the Victim Board	137
Brute-Forcing Secure Boot Loaders in Power-Analysis Attacks	138
Prepping Your Test with AVRDUDESS	139
Setting Up the ChipWhisperer for Serial Communications	140
Setting a Custom Password	141
Resetting the AVR	143
Setting Up the ChipWhisperer ADC	143
Monitoring Power Usage on Password Entry	145
Scripting the ChipWhisperer with Python	147
Fault Injection	148
Clock Glitching	148
Setting a Trigger Line	154
Power Glitching	156
Invasive Fault Injection	156
Summary	156

9 IN-VEHICLE INFOTAINMENT SYSTEMS 157

Attack Surfaces	158
Attacking Through the Update System	158
Identifying Your System	159
Determining the Update File Type	160
Modifying the System	161
Apps and Plugins	163
Identifying Vulnerabilities	164
Attacking the IVI Hardware	166
Dissecting the IVI Unit's Connections	166
Disassembling the IVI Unit	168

Infotainment Test Benches	170
GENIVI Meta-IVI	170
Automotive Grade Linux	173
Acquiring an OEM IVI for Testing	174
Summary	175

10
VEHICLE-TO-VEHICLE COMMUNICATION **177**

Methods of V2V Communication	178
The DSRC Protocol	179
Features and Uses	180
Roadside DSRC Systems	181
WAVE Standard	184
Tracking Vehicles with DSRC	186
Security Concerns	186
PKI-Based Security Measures	188
Vehicle Certificates	188
Anonymous Certificates	189
Certificate Provisioning	189
Updating the Certificate Revocation List	191
Misbehavior Reports	192
Summary	192

11
WEAPONIZING CAN FINDINGS **193**

Writing the Exploit in C	194
Converting to Assembly Code	196
Converting Assembly to Shellcode	199
Removing NULLs	199
Creating a Metasploit Payload	200
Determining Your Target Make	202
Interactive Probing	203
Passive CAN Bus Fingerprinting	204
Responsible Exploitation	208
Summary	208

12
ATTACKING WIRELESS SYSTEMS WITH SDR **209**

Wireless Systems and SDR	210
Signal Modulation	210
Hacking with TPMS	211
Eavesdropping with a Radio Receiver	212
TPMS Packets	213
Activating a Signal	214
Tracking a Vehicle	214

Event Triggering	214
Sending Forged Packets	215
Attacking Key Fobs and Immobilizers	215
Key Fob Hacks	216
Attacking a PKES System	219
Immobilizer Cryptography	220
Physical Attacks on the Immobilizer System	228
Flashback: Hotwiring	230
Summary	231

13 PERFORMANCE TUNING 233

Performance Tuning Trade-Offs	234
ECU Tuning	235
Chip Tuning	236
Flash Tuning	238
Stand-Alone Engine Management	239
Summary	240

A TOOLS OF THE TRADE 241

Hardware	241
Lower-End CAN Devices	242
Higher-End CAN Devices	245
Software	246
Wireshark	246
PyOBD Module	246
Linux Tools	247
CANiBUS Server	248
Kayak	248
SavvyCAN	248
O2OO Data Logger	249
Caring Caribou	249
cOf Fingerprinting Tool	250
UDSim ECU Simulator	250
Octane CAN Bus Sniffer	250
AVRDUDESS GUI	251
RomRaider ECU Tuner	251
Komodo CAN Bus Sniffer	251
Vehicle Spy	252

B DIAGNOSTIC CODE MODES AND PIDS 253

Modes Above 0x10	253
Useful PIDs	254

C	
CREATING YOUR OWN OPEN GARAGE	255
Filling Out the Character Sheet	255
When to Meet	257
Affiliations and Private Memberships	257
Defining Your Meeting Space	258
Contact Information	258
Initial Managing Officers	259
Equipment	259
 ABBREVIATIONS	 261
 INDEX	 263