Tobias on Locks and Insecurity Engineering

Tobias828259_ffirs.indd 1 1/8/2024 2:35:31 PM

Tobias828259_ffirs.indd 2 1/8/2024 2:35:31 PM

Tobias on Locks and Insecurity Engineering

Understanding and Preventing Design Vulnerabilities in Locks, Safes, and Security Hardware

Marc Weber Tobias, J.D.

Member of ASIS, ALOA, SAVTA, IAIL,
FBI InfraGard, AAPP, and APA;
technical advisor to AFTE; and
member of the Underwriters Laboratory Standards
Technical Panel on Locks and Safes

WILEY

Tobias828259_ffirs.indd 3 1/8/2024 2:35:31 PM

Copyright @ 2024 by Marc Weber Tobias, J.D. All rights reserved.

Published by John Wiley & Sons, Inc., Hoboken, New Jersey.
Published simultaneously in Canada and the United Kingdom.

ISBNs: 9781119828259 (Hardback), 9781119828631 (ePDF), 9781119828266 (ePub)

No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning, or otherwise, except as permitted under Section 107 or 108 of the 1976 United States Copyright Act, without either the prior written permission of the Publisher, or authorization through payment of the appropriate per-copy fee to the Copyright Clearance Center, Inc., 222 Rosewood Drive, Danvers, MA 01923, (978) 750-8400, fax (978) 750-4470, or on the web at www.copyright.com. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Inc., 111 River Street, Hoboken, NJ 07030, (201) 748-6011, fax (201) 748-6008, or online at www.wiley.com/go/permission.

Trademarks: WILEY and the Wiley logo are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates, in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. John Wiley & Sons, Inc. is not associated with any product or vendor mentioned in this book.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. No warranty may be created or extended by sales representatives or written sales materials. The advice and strategies contained herein may not be suitable for your situation. You should consult with a professional where appropriate. Further, readers should be aware that websites listed in this work may have changed or disappeared between when this work was written and when it is read. Neither the publisher nor author shall be liable for any loss of profit or any other commercial damages, including but not limited to special, incidental, consequential, or other damages.

For general information on our other products and services or for technical support, please contact our Customer Care Department within the United States at (800) 762-2974, outside the United States at (317) 572-3993 or fax (317) 572-4002.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic formats. For more information about Wiley products, visit our web site at www.wiley.com.

Library of Congress Control Number: 2023946543

Cover images: Vault: © mennovandijk/Getty Images
Lights: © Tatiana Serebryakova/Getty Images
Circuit Board: © DKosig/Getty Images
Cover design: Wiley

For Addi Wendt, one of the modern pioneers in the lock and security industry and a dear friend. He dedicated his life to developing and providing tools and advanced opening techniques for locksmiths and government services worldwide. And to the memory of Betty Mae Tobias, my beloved mother, who continually encouraged me to write this book before her passing.

Tobias828259_ffirs.indd 5 1/8/2024 2:35:32 PM

Tobias828259_ffirs.indd 6 1/8/2024 2:35:32 PM

About the Author

Marc Weber Tobias J.D., is an investigative attorney and a physical security expert. His undergraduate major and degrees were in law enforcement and journalism, and he received his Juris Doctor degree from Creighton Law School in 1973.

He has authored seven law enforcement textbooks, including *Locks, Safes, and Security: An International Police Reference,* first and second editions, and *LSS+* (the Multimedia Edition). This is a primary reference for law enforcement, intelligence, locksmiths, and professional security officers.

He has contributed to Forbes for 12 years on matters of travel and security and has disclosed serious vulnerabilities in lock designs.

Marc has been granted 28 U.S. patents and has lectured worldwide on criminal investigations, liability, locks design, and bypass tools and techniques.

During his career, he has worked for government agencies as an investigator and prosecutor of major crimes. He and his colleagues also consult for many of the major lock manufacturers in the United States, Europe, and the Middle East. He directs a team that discovers vulnerabilities that can compromise the locks produced by his clients and then works with their design engineers to fix them.

Marc established the Security Engineering Laboratory at the University of Pittsburgh, School of Engineering, where senior engineering students work on security-related product designs.

He is a member of many professional organizations, including the Associated Locksmiths of America (ALOA), Safe and Vault Technicians Association (SAVTA), American Society for Industrial Security (ASIS), International Association of

Tobias828259_ffirs.indd 7 1/8/2024 2:35:33 PM

Investigative Locksmiths (IAIL), American Association of Police Polygraphers (AAPP), American Polygraph Association (APA), Underwriters Laboratory Standards Technical Panel, and FBI InfraGard. He is a technical advisor to the Association of Firearms and Tool Marks Examiners (AFTE), the professional crime lab and forensic organization for law enforcement agencies worldwide.

Marc and his partners lectured at DefCon and other major cyber conferences for nine years on physical security, lock designs, and vulnerabilities. He has consulted with many law enforcement organizations and testified as an expert witness involving crimes related to the bypass of locks, including the major diamond theft in Antwerp, Belgium, and several homicide cases.

Books by the Author

A Field Manual of Criminal Law and Police Procedure, by Marc Weber Tobias and R. David Petersen, 1975

Locks, Safes, and Security, First Edition, 1970

Locks, Safes, and Security, Second Edition, 2000

Locks, Safes, and Security: The Multimedia Edition LSS+, 2002

Open in Thirty Seconds: Cracking One of the Most Secure Locks in America, by Marc Weber Tobias and Tobias Bluzmanis, 2008

Police Communications, 1974

Pre-Trial Criminal Procedure, by Marc Weber Tobias and R. David Petersen, 1972

Techno Security's Guide to Securing SCADA: A Comprehensive Handbook on Protecting the Critical Infrastructure, 2008

Tobias828259_ffirs.indd 9 1/8/2024 2:35:33 PM

Tobias828259_ffirs.indd 10 1/8/2024 2:35:33 PM

Acknowledgments

I would like to acknowledge the following people for helping to influence me in the writing of this book. The journey took me to many different countries to meet with specialists in locks, safes, and cybersecurity while making many friends along the way.

First, I'd like to thank the experts who have provided the most influence. Thank you to John Falle (Falle Safe Security); Enrico and Sascha Wendt (Lockmasters Germany); Alexandre Triffault (AT Security); Andreas Haberli (dormakaba); Clyde Roberson and Peter Field (Medeco); Eliot Springer (Israel Intel-Research and the New York Police Department [NYPD]); Lt. Mike Bach (NYPD TARU Unit); Graham Pulford; Harry Sher; Jacques Pyronnet; Jose Luis (Vicuna Tools); Juergen Kruehn (Ikon); Kloppers Burgert (South Africa Police Commander); Rami Almosnino, Nava Efrati, and Sam Shterenshus (MUL-T-LOCk); Eric Winter (University of Pittsburgh); David Moser, Torsten Quast, and Han Fey (ASSA ABLOY); Javier Roquero; Marc Handels and Juan Imedio (SaltoSystems Team); S. Ehlich-Adam (EVVA Locks); Urs Spani (KESO Locks); Bo Widen (inventor extraordinaire, Sweden); and Klaus Drumm (Geminy Locks).

Special recognition to Dr. Roger G. Johnston, Ph.D., retired Vulnerability Assessment team leader at Los Alamos and Argonne National Laboratories, for his insight into security and keeping America safe.

Second, my appreciation is given to Ross Anderson and the University of Cambridge for his expertise in cybersecurity and friendship, and Clayton Miller of Lockmasters (United States). Thanks also goes to Manfred Goth (Goth Forensic Laboratory), Nasser Al-Shamshi (Dubai Police Crime Lab), Tzachi Wiesenfeld, Tammy and Paul Davis (Videx), Vito Ruscigno (Italian Police inspector), and Jay Dean Smith (Denver Police Department).

Tobias828259_ffirs.indd 11 1/8/2024 2:35:33 PM

Third, I thank all the lock innovators and creators for their covert-entry tool designs. Thanks also goes to Frederick Madelin (Madelin S.A.), Martin Newton (Safe Ventures in the UK), and Roy Saunders, the world's best safecracker (England).

Finally, my sincere thanks goes to those in the industry who helped make this book possible. Thank you sincerely to Dr. Alejandro Ojeda (Urban Alps), Aaron Fish, Barry Wels, Brock Self, Cedric Messequer, The Czech Locksmith Association, The European Locksmith Federation and Ona Gardemeister, Eric Michaud, Graham Pulford, Hans Milejeda, Harry Sferopoulos, Dr. Ilya Zeldes, Isabel Chernoff, Jacques Pyronnet, Jeff Proehl, Jean Marie Machefert, Jimmie Oxley and the University of Rhode Island, John Jackson, Mark Bloom (Spectrum Brands), Mary Besterfield-Sacre (Associate Dean, School of Engineering, University of Pittsburgh), Michael and Jane Tobias, Ralph Vasami (Builders Hardware Manufacturing Association), Reuven Borokovsky (Mul-T-Lock), and Governor William J. Janklow (South Dakota).

Finally, my colleague and co-conspirator, Tobias Alberto Bluzmanis, was invaluable because of the lock investigations we conducted, his brilliance as a locksmith, and the many patents we have received over the years. My work would have been impossible without Toby's ideas, input, and creativity.

Contents at a Glance

Foreword		xxxiii
Introduction		xxxv
Part I	Locks, Safes, and Insecurity Engineering	1
Chapter 1	Insecurity Engineering and the Design of Locks	3
Chapter 2	Insecurity Engineering: A Lack of Expertise and Imagination	25
Chapter 3	Vulnerability Assessment in Lock Designs	49
Chapter 4	The 3T2R Rule for Assessing the Security of a Lock	67
Part II	Legal and Regulatory Issues in Locks, Safes, and Security Systems	87
Chapter 5	Security Is All About Liability	89
Chapter 6	Legal Liability and Insecurity Engineering	103
Chapter 7	Standards for Locks and Safes	131
Chapter 8	Patents, Security, and the Protection of Intellectual Property	163
Chapter 9	Notification of Defects in Product Design	187
Chapter 10	Legal and Security Issues in Keying Systems	209
Part III	Basic Designs and Technologies for Mechanical and Electronic Locks	231
Chapter 11	A Brief History of Lock Design and Development	233
Chapter 12	Industry Definitions	257

Tobias828259_ftoc01.indd 13 1/8/2024 2:35:25 PM

Chapter 13	Modern Locking Mechanisms: A Merging of Old and New Technology	279
Chapter 14	A Comparison of High-Security Lock Designs	317
Part IV	Design and Insecure Engineering of Locks	339
Chapter 15	Attacks Against Locks: Then and Now	341
Chapter 16	An Overview: Vulnerability Analysis in Designs and Testing	379
Chapter 17	Destructive Attacks Against Locks and Related Hardware	395
Chapter 18	Covert Methods of Entry	417
Chapter 19	Attacks Against Electronic Locks	445
Chapter 20	Advanced Attacks Against High-Security Locks	459
Part V	Attacks on Key Control and Special Keying Systems	475
Chapter 21	Attacking Keys and Keying Systems	477
Chapter 22	Advanced Attacks on Key Control: 3D Printers and Special Software	507
Chapter 23	Digital Fingerprints of Locks: Electronic Decoding Systems	523
Chapter 24	Code-Setting Keys: A Case Study of an Attack on High-Security Key Control	537
Part VI	Specific Case Examples	545
Chapter 25	Case Examples from Part VII Rules	547
Chapter 26	Case Examples By Category	571
Part VII	Design Rules, Axioms, and Principles	597
Chapter 27	Design Rules, Axioms, and Guidelines	599
Epilogue		625
Appendix A	Patents Issued	627
Appendix B	Trademark Listing	629
Index		633

Contents

Foreword		**xxxiii**
Introduction		**xxxv**
Part I	**Locks, Safes, and Insecurity Engineering**	**1**
Chapter 1	**Insecurity Engineering and the Design of Locks**	**3**
	What Is Insecurity Engineering?	4
	Primary Responsibilities of Lock Manufacturers	4
	Invent or Improve On State-of-the-Art Technology	5
	Develop and Continue to Analyze and Improve On Earlier Designs	5
	Understand All Known Vulnerabilities and Imagine New Ones	6
	Apply Expertise to Currently Manufactured and New Products	6
	Protect Intellectual Property (IP) from Infringement	6
	Ensure That IP Produced and Sold Is Secure and Will Not Cause Injury or Harm	6
	Do Not Produce Defective Products	6
	Fully Understand Product Liability and Its Critical Importance	7
	Initiate a Disclosure Program about Serious Vulnerabilities	7
	Examples of Insecurity Engineering Failures	7
	Important Design Rules	18
	Summary	24
Chapter 2	**Insecurity Engineering: A Lack of Expertise and Imagination**	**25**
	Basic Lock Types and Components	29
	Theory of Operation for Each Primary Lock Design Category	29
	Primary Security Classifications of Locks	31
	Lock Materials and Their Characteristics	33
	Standards and Their Criteria	34
	Security Features and Enhancements	34

Tobias828259_ftoc.indd 15 1/8/2024 2:35:19 PM

Magnetics: Theory, Implementation, and Defeat 35
Bypass: Fundamental Expertise Requirements 35
Mechanical Bypass of Locks and Systems 36
Brute-Force Attacks 37
Traditional Covert Entry 38
Picking 38
Impressioning 39
Decoding 40
Hybrid Attacks 42
Keys and Keying Systems and Their Design and Compromise 42
Attacks Against Shear Lines 44
Forensics and Evidence of Entry 45
Evidence of Entry 46
Audit Trails 46

Chapter 3 Vulnerability Assessment in Lock Designs 49
Vulnerability and Risks 51
Defining a Vulnerability Assessment Plan 52
VA Team Selection 53
The Vulnerability Assessment Process 57
Insider Threats and Attacks 59
Vulnerability Assessment Report 59
Suggested Rules, Axioms, Guidelines, and Principles 61

Chapter 4 The 3T2R Rule for Assessing the Security of a Lock 67
The 3T2R Rule: Metrics, Security, and Liability 68
Time 68
Various Time Computations and Attack Vector Examples 69
Time Delay, Security, and Liability 72
Tools 72
Forced Entry 73
Covert and Surreptitious Entry 73
Hybrid Attacks and the 3T2R Rule 75
Tool Assessment and the 3T2R Rule: Simple, Complex, or Special Designs 77
Training 79
Reliability of the Exploit 81
Repeatability of the Exploit 81
Overall Security Assessment and the 3T2R Rule and Numerical Scoring 82
Security Ratings for Simple or Complex Attacks: Case Examples 83

Part II Legal and Regulatory Issues in Locks, Safes, and Security Systems 87

Chapter 5 Security Is All About Liability 89
Avoiding Legal Issues 89
Design Defects and Other Actions as the Basis of Product Liability 90

Design Defect Liability 90
How to Define Defectiveness 91
Fraud and Misrepresentation 91
False Representations 92
Failure to Warn of a Dangerous Condition 92
Failure to Foresee Product Use and Subsequent Liability 93
Post-Sale Failure to Warn 93
Post-Sale Duty to Remedy a Defect or Recall 94
Failure to Disclose or Warn of a Known Defect 95
Failure to Design Away Known Defects or Dangers 95
Misconduct in Marketing 96
Tortious Misrepresentation about a Product 96
Failure to Adhere to Industry Standards, Cutting Corners, or Falsifying Test Results 96
Negligence in Design or Manufacture, or Failure to Provide Adequate Warnings or Instructions 97
Failure to Implement a Risk-Utility Test in Product Design 97
Failure to Consider Alternative Designs 97
Malfunctions and Liability 98
Flagrant Disregard of Consumer Safety 98
Failure to Exercise Due Care in Manufacturing 98
Failure of a Manufacturer to Exercise Reasonable Care in Product Concept and Formulation 99
Defective Product or Improper Consumer Use 99
Summary of Specific Actions That Can Trigger Liability and Legal Issues 99
Failure to Discourage a Culture of Arrogance in Engineering and Design 100

Chapter 6 Legal Liability and Insecurity Engineering 103
Development of Product Liability Law 104
Criminal, Civil, and Criminal Law 105
Overview: Origins of Legal Liability for Product Designs 105
Ancient Roman Law and the Twelve Tables 106
The Emergence of a Standard of Care and an Extra-High Standard 106
Privity of Contract: The Case of *Winterbottom v. Wright* 108
Privity of Contract and Avoidance of Liability by Manufacturers: Implied Warranty Claims 109
Defective Products: What Are They, and Why Are They Important? 110
Manufacturing Defects 111
Design Defects 112
Warning and Marketing Defects 113
Post-Sale Issues and Duty to Warn 114
Exemption from Warnings: Sophisticated Users 114
Warranty of Merchantability, Defective Products, and Negligence 115

The Repair Doctrine: Liability for Subsequent Product Upgrades 116
Negligence vs. Privity of Contract 117
MacPherson v. Buick Motor Car Company 117
Strict Liability vs. Negligence 118
Strict Liability 118
Who Can Sue for a Defective Product? Horizontal and Vertical Privity 119
The Malfunction Doctrine and a Defective Product 119
Failure to Implement an Alternative Design and Proof of Possibility 120
Risk-Utility Analysis of an Alternative Product Design 120
Knowingly Selling a Defective Product 121
User Misconduct Defenses 122
Liability for Misuse of a Product 123
State-of-the-Art or Defective? 124
Manufacturers Are Experts 126
Reasonable Foreseeability 127
Constructive Knowledge of Risk 127
Due Care in Manufacturing 127
Due Care in Design 127
Industry Standards and Proof of Negligence 128
Elements of Proof by a Manufacturer 128
Elements of Proof by a Plaintiff 128
Liability for Nonmanufacturers and Retailers 129
Fraudulent or False Misrepresentation 129

Chapter 7 Standards for Locks and Safes 131
Basic Rules and Axioms Relating to Standards 133
U.S. Standards Organizations 137
Underwriters Laboratory 137
Builders Hardware Manufacturers Association 138
American Society for Testing and Materials 138
Description and Analysis of U.S. Lock Standards: UL and BHMA 139
UL 437: The Commercial Security Standard 139
UL 437 Definitions and Test Requirements 139
Attack-Resistance Times for Door Locks (Section 11.5) 141
BHMA/ANSI 156.30 High-Security Standard 142
Section 5: Key Control 143
Section 6: Destructive Testing 144
Section 7: Surreptitious-Entry Resistance 144
BHMA 156.5 Cylinders and Input Devices for Locks 146
Operational Tests Before and After Cycle Tests 146
Cycle Test 147
Strength Tests 147
Electrified Input Devices 148

Deficiencies in the UL 437, BHMA 156.30, and 156.5 Standards 148
UL 437 Failures to Identify Vulnerabilities and Issues in Testing Protocols 148
Key Control 149
Pick, Bumping, and Impressioning Resistance 149
Complex Forms of Picking 150
Expertise Level of Those Performing Tests 151
Forced-Entry Resistance 151
Reliance on UL Standards: No Liability 151
Bump Keys 152
Decoding Attacks 152
Key Control and 3D-Printed Keys 153
Testing Deficiencies in the BHMA 156.30 Standard 153
Forced Entry 153
Mechanical Bypass of Locking Mechanisms 154
Audit Trail for Electronic Locks 155
Keys and Key Control 155
Decoding 156
Data From Within the Lock 157
Data From Sources Outside the Cylinder 157
Pick Resistance 158
Exploit of Internal Tolerances 158
Electronic Attacks and Testing 159
Tools Commercially Available to Locksmiths 159
Bumping and Rapping Resistance 160
Recommendations for a High-Security Standard 160

Chapter 8 Patents, Security, and the Protection of Intellectual Property 163
Patents and Their Relationship to the Security of an Invention 165
Modifications to Existing Patented Products and Security 166
History, Origins, Chronology, and Rationale for Patent Laws 166
Relevant International Patent Treaties 167
Paris Convention for the Protection of Industrial Property 168
Patent Cooperation Treaty 168
TRIPS Agreement: Trade-Related Aspects of Intellectual Property 168
Overview: Current U.S. Patent Law 169
The Definition of an Invention 170
Types of Patents 170
Utility Patents 170
Design Patents 170
Plant Patents 171
Patent Rights and Their Value 171

Filing and Obtaining a Patent in the United States 172
Provisional Applications 172
Nonprovisional Applications 172
Critical Steps to Take Before Filing a Nonprovisional Application 173
Specific Legal Filing Requirements 173
Proper Naming and Identification of the Inventor 174
Primary Parts of a Patent Application 175
Specification 175
Claims 175
Primary Statutory Criteria for the Issuance of a Patent 176
Utility 176
Novelty 177
Nonobviousness 177
Patent Life and Validity 178
What Patent Rights Do Not Cover or Allow 178
Invalidation of a Patent Application: The Concept of Prior Art and Nondisclosure of Inventions 179
Filing for a Patent to Protect IP: Pros and Cons 181
Advantages of Filing an Application 181
Reasons Not to File an Application 182
Patent Searches and Tools 182
Patent Classification System 183
Patent Infringement 183
Summary of Criteria That Constitute Infringement 184
Direct Infringement 184
Indirect or Dependent Infringement 184
Defenses to Infringement Actions 185
Civil and Criminal Remedies for Infringement 186

Chapter 9 Notification of Defects in Product Design 187
Primary Rules and Questions 188
Internal Notifications 193
Assessing the Scope of the Issue or Problem 194
Action Items and Priority 195
Design Defects and Liability Considerations 195
Compensatory and Punitive Damages 197
Failure to Take Any Substantive Steps 197
Post-Sale Duty to Warn or Recall 197
The Protocol for the Notification of Defects in Locks 198
Threat-Level Criteria 198
Communications and Actions on Notification of a Defect 200
Special Cases: Consulting Agreements, Nondisclosure Agreements, and Extortion Attempts 201
Possible Extortion Attempts 202
Civil Remedies 204
Insider Threats as Part of a Scheme 207

Chapter 10 Legal and Security Issues in Keying Systems 209
How Manufacturers and Locksmiths Can Be Liable for Damages 210
False or Misleading Advertising About Security and Key Control 211
Key Control Procedures by Manufacturers 212
How Locksmiths and Key-Duplicating Shops Can Defeat Key Control Schemes 213
Cutting Keys on Counterfeit, Knockoff, or Legally Restricted Blanks 214
Legal Restrictions 215
Patent Infringement 215
Contract Violation by Dealers 215
Voiding of Warranty 215
Potential Violation of City Ordinances 216
Identification of Counterfeit Blanks by Customers 216
Patent-Expired Blanks 216
Keyway Restrictions Are Often Easily Circumvented 216
Compromise of Physical Key Control: Duplication, Simulation, and Replication of Credentials 217
Duplication 218
Sophisticated Computerized Key Machines 218
Milling Machines 219
3D Printers and Key Machines 219
Simulation 220
Visual Decoding of Keys 220
Variable Key-Generation Systems 221
Dimple Key Simulation and Overlay Bitting Insert 221
Replication 222
Decoding 222
Impressioning 222
Rights Amplification 223
Inadequate Number of Differs 224
Pinning Restrictions and Maximum Adjacent Cut Specifications 224
Extrapolation of Top-Level Master Keys 225
Defeat of Virtual Keyways 225
Creation of Bump Keys and Lock Bumping 225
Legal Issues in Master Key Systems 226
Extrapolation of Top-Level Master Keys 228
Systems Protected by Side Bit Milling and Sidebar Codes 228
Analysis of Multiple Keys in a System to Derive a Pattern or Sequence of Bitting 229
Analysis of Many Keys in a Positional Master Keying System to Derive the Composite Master Key Code 229
Security Policies for Organizational Key Control 229

Part III Basic Designs and Technologies for Mechanical and Electronic Locks 231

Chapter 11 A Brief History of Lock Design and Development 233
From Blacksmiths to Locksmiths: The Development of the Technology of Locks 234
The First Locking Systems 235
The Original Egyptian Pin Tumbler Design 237
Early Roman Locks and the Introduction of Wards 239
Lock Designs in the Middle Ages: The Introduction of the Lever Tumbler 242
Advancements in Lever Lock Designs 244
Robert Barron: Double-Acting Lever Tumbler 244
The Bramah Lock: No Direct Contact Between the Key and Bolt Mechanism 245
The House of Chubb and the Detector Lock 246
Parsons Balanced Lever Lock 247
Newell Parautoptic Lock 247
Hobbs Protector Lock 248
Tucker and Reeves Safeguard Lock 249
Yale Pin Tumbler Lock 250
Disc Tumbler Lock 252
Wafer Tumbler Lock 253
Sidebar Locks: Briggs & Stratton 255
Advancements in the Past 50 Years 255

Chapter 12 Industry Definitions 257
Terminology 258

Chapter 13 Modern Locking Mechanisms: A Merging of Old and New Technology 279
Conventional Mechanical Locks 283
Wafer Tumbler Locks 284
Hybrid Wafer Lock Designs with Sidebars 286
Rotating Disc Designs 288
Pin Tumbler Locks 288
Components and Fundamental Operating Principles of a Conventional Pin Tumbler Lock 289
Security Vulnerabilities of Conventional (and Some High-Security) Pin Tumbler Locks 291
Hybrid Mechanical Designs 294
Sidebars 294
Dimple Locks and Telescoping Pins 294
Axial Pin Tumblers 296
Laser-Track Combinations 296
Rotating Pin Tumblers and Sidebars 296
Magnetic Fields and Rotating Discs 299

Security Enhancements to Conventional Locks 300
Anti-Drill Pins and Barriers 300
Blocking Access through the Keyway 300
Anti-Bumping Pins 301
Security Pins and False Gates or Notches 301
Bitting Design 301
High-Security Mechanical Locks 302
Attributes of High-Security Locks 304
Software- and Hardware-Based Keys, Locks, and Access Control 305
Key-Based Digital Cylinders 305
Assa Abloy CLIQ 306
Assa Abloy eCLIQ 306
Energy-Harvesting Locks 307
iLOQ 308
Abloy Pulse, eCLIQ, and Spark 310
Electronic Locks 310
Hybrid Electronic Locks with Biometric or Wireless Authentication 311
Kwikset KEVO 311
Wireless Door Locks, Access Control, and Authentication 312
Selecting Conventional or High-Security Locks 315

Chapter 14 A Comparison of High-Security Lock Designs 317
Criteria for Judging a Lock's Security 318
Sidebars and Secondary Locking Systems 319
Side Bit Milling and Sidebars 320
Assa Twin, V10, and Similar Sidebar Designs 321
Unique Finger Pin Design 322
Side Pins: Two Contact Points 322
Sidebar Interaction with Side Pins 323
Schlage Primus 324
Primus Sidebar and Finger Pin Design 325
Medeco Rotating Tumbler Sidebar Design 326
Original Medeco Designs 328
Medeco BIAXIAL 328
Medeco m3 328
Medeco M4: The Latest Adaptation of Side Bit Milling 332
EVVA Magnetic Code System (MCS) 334

Part IV Design and Insecure Engineering of Locks 339

Chapter 15 Attacks Against Locks: Then and Now 341
The Origins of the Pin Tumbler Lock and Attacks on Its Security 344
Warded Lock Design and Insecurity 346
Multiple Bolts for Warded Locks 347
Methods of Entry for Warded Locks 347

Skeleton Keys and Entry Tools 349
Impressioning Techniques for Warded Locks 350
Picking Tools for Warded Mechanisms 351
Special Programmable Keys for Warded Locks 353
Lever Tumbler Locks 353
Trap for False Keys 355
Methods of Attacks Against Lever Locks 355
Belly Decoding with Plasticine or Other Materials 356
False Keys or Key Copies with Wax and Permutating Key Machines 357
Early Impressioning Techniques 357
Mapping the Tumblers to Determine Measurement 358
Mapping the Tumblers with Printer's Ink 359
Methods of Picking Lever Locks 359
KGB Programmable Lever Lock Key Set 360
Overlifting Tumblers 360
Decoding Through Belly Reading 362
Opening Letter Locks 363
Mechanical and Arithmetic Attacks and Tryout Keys 363
The Fenby Permutating Key-Cutting Machine 364
Serrated Notches and Security Pins 364
Expanding Bits on Keys 364
Small Keyhole Preventing the Exertion or Use of Force from Tools 365
Barrel and Curtain Used to Restrict Access to Internal Mechanisms 365
Pressure Against the Bolt 366
The Great Exhibition of 1851, Hobbs, and the Insecurity of Locks 366
Lock-Picking Advances in England and America: Nineteenth Century 366
Bramah Lock Design 367
Attacks with Explosives 368
Forced Attacks with Special Tools 369
Decoding Lever Locks by Sound 369
Major Crimes Involving Locks During the Nineteenth and Twentieth Centuries 370
The Great Train Robbery of 1855 370
The Antwerp Diamond Heist of 2003 370
1950 Brinks Robbery in Boston 370
Attacks on Locks: The Past 100 Years 371
Attacks on Locks: Now and in the Future 373

Chapter 16 An Overview: Vulnerability Analysis in Designs and Testing 379
Primary Components in All Locks 380
Shell or Housing 380
Plug and Keyway 381

Keys or Credentials 381
Shear Line 381
Gates and Sidebars 383
Movable Locking Components 383
Secondary Security Components for Multiple Security Layers 384
Assembly-Retaining Components 384
Motion Transfer Components for Movement of Bolts, Latches, or Blocking Elements 384
Mechanical Electronic Interface 384
Primary Classification of Attack Types 385
Traditional Forced Attacks 385
Hybrid Forced Actions 386
Covert Attacks 387
Shear-Line Attacks 387
Attacks Against Internal Tolerances 387
Attacks Against Physical Integrity 388
Decoding Attacks Against Mechanical Credentials 388
Attacks Against Keys and Bitting 388
Attacks Against Lock Assembly and Bolt Mechanisms 389
Attacks Against Systems That Control External Locking Elements 389
Attacks Against Any Openings 389
Magnetic Fields 389
Covert Hybrid Attacks Against Mechanical Locking Elements 390
Special Hybrid Attacks to Neutralize Individual Security Layers 390
Covert Forced Hybrid Attacks 391
Hybrid Attacks Against Detainers 391
Unintended Consequences 391
Digital Door Lock Designs 391
Biometric Access to Gun Safes and Secure Containers 392
Bumping and Rapping 392
Bypass of Reset Buttons 392
Defeating Audit Trails in Electromechanical Locks 392
Keyway Access to the Latch or Bolt 392
Nitinol Wire Design Defect in Merchandise Display Case Locks 393
USB Data Port Access in Electronic Locks 393
Magnetics and Electronic Laptop Locks 393
Copying Defective Designs 393
Newton's Laws of Motion 394
Ratchet Mechanisms and Shims 394
Use of Plastics in Lock Designs 394
Vibration and Failure to Use Springs 394

Chapter 17 Destructive Attacks Against Locks and Related Hardware 395
Tools, Techniques, and Threats from the Application of Different Forces 396
Shearing, Sawing, or Cutting 396
Drilling 396
Creating a Shear Line 399
Drilling and Pulling Attacks on Profile Cylinders 401
Pounding, Driving, Prying, and Fracturing Materials 403
Bending 404
Torsion or Twisting 405
Torque, Wrenching, Leverage, Jimmying, and Wedging Against Components 405
Opposing Forces Applied Simultaneously: Breaking, Prying, Wedging, Peeling, Ripping, and Spreading 406
Compression and Shearing Force 411
Impact, Blows, Shock, Hydraulic-Pneumatic Pressure, and Compressed Air 411
Bouncing or Bumping of Locking Components 411
Battering-Ram Door Hammer 411
Slam Hammer 412
Punching 412
Chisel and Wedging 412
Application of Temperature Extremes 412
Chemical Attacks Against Internal Components 414
Basic Tools of Destructive Entry 414

Chapter 18 Covert Methods of Entry 417
Covert Entry: The Fundamental Premise 418
Primary Points of Vulnerability for All Locks 419
Assessing and Choosing Methods of Attack 420
Covert-Entry Methods 421
Shear Line Attacks 423
Picking 423
Impressioning 436
Variable Key-Generation System 438
Magnetic Attacks 440
Processor Reset Attacks 441
Decoding Information from Within the Lock 441
Audio Frequencies and Sound 442
Piezo Measurement 442
Feeling, Friction, and Decoding 442
Belly Reading and Markings 443
Against Any Openings into the Lock Body with Shims and Wires 443

Chapter 19 Attacks Against Electronic Locks 445
Electronic-Based Locks: Common Design Vulnerabilities and Attacks 447

Bumping and Rapping to Move Rotors 447
Attacks Against Electronic Elements Blocking Movement 448
Rotor Manipulation by Application of Energy 449
Piggyback Attacks 450
Replicating the Original Mechanical Key Bitting 451
A Modified Piggyback Attack: Drilling to Create Access to the Motor 451
Magnetic Fishing and Shim-Wire Movement 452
Direct Electrical Access to the Motor 453
Auto Reset of Relock Exploit 453
Exploiting Reset Functions in Electromechanical Locks 454
Drilling for Rotor Access 454
Drilling to Force the Sidebar to Retract 455
Potential Design Vulnerabilities to Review 455

Chapter 20 Advanced Attacks Against High-Security Locks 459
Considerations in Developing Attack Strategies, Techniques, and Tools 460
Unique Design Approaches to Opening Lever and Pin Tumbler Locks 464
Pin and Cam Systems 464
The Universal Belly Reader 466
Pin-Lock Pin and Cam Systems 466
Systems Based on the Use of Shims 467
The Basic Pin-Lock Decoder 467
Core-Shim Decoder 468
The Medeco BIAXIAL Shim Decoder 469
Material Impressioning System 469
Foil Impressioning System 470
Impressioning Lightbox 471
Plasticine Reading Systems 471
Variable Key-Generation Systems 472
The Universal Pin Tumbler Variable Key System 472
Reusable Variable Key Systems 472

Part V Attacks on Key Control and Special Keying Systems 475

Chapter 21 Attacking Keys and Keying Systems 477
Summary of Attack Strategies Against Keys, Plugs, and Detainers 478
Intelligence from Locks and Keyways 479
Lock Manufacturer 481
Signature of the Keyway 481
Special Industry Keys and Identification Data 481
Key Codes and Other Data Stamped on Keys 482
The Key's Physical Design 482
The Key's Bitting Data 482
Movable Elements 482
The Number of Pin Tumblers, Discs, or Wafers 483

Correlation Between Physical Key Design and Master Key Systems 483
Depth and Spacing 484
Decoding Depth and Spacing Information 485
Manufacturer-Imposed Rules About Bitting and Key Codes 487
Information Appearing on the Lock Face 487
Master Keys and Keying Progression 488
Secondary Locking Systems 488
Sectional Keyways and Counterfeit Blanks 488
Maison Keying Systems 488
Photographing or Scanning Keys for Later Reproduction 488
Restricted Keyways 489
Attacks Against Keying Systems 489
Rights Amplification of Keys and Locks 489
Recutting a Key to Change the Bitting 490
Modification of Keyway Warding 490
Altering Virtual Keyway Systems 490
Modifying the Secondary Locking System 491
Inserting an Overlay into a Blank or Cut Key 491
Converting a Change Key to a Blank Key 491
Creating a New Shear Line 491
Replicating or Copying a Target Key 492
Generating System Keys 492
Extrapolation of the Top-Level Master Key 493
Secondary Locking System Decoding 493
Creating Bump Keys 493
Decoding Control Keys 493
Mechanical Bypass 494
Compromise of Key Control Procedures 495
Tryout Keys 496
Exploiting Key-Interchange Issues and Tolerances 496
Defeating Virtual Keyways 497
Defeating Ferrous Elements with Magnetic Fields 497
Incidental Master Keys, Online Key Information, and Electronic Credential Cloning 497
Compromising the Master Key Other than by Extrapolation 498
Physically Copying, Photographing, or Decoding a Master Key 498
Accessing One or More Cylinders to Decode the Pin Segments 498
Using a Falle Pin-Lock Decoder to Measure Pin Segments Using Shim Wires 498
Falle Pin and Cam Decoder 498
Shimming the Cylinder with Depth Keys 499
Visual Inspection of Bitting Values 499
Viewing Tumblers, Discs, Wafers, or Active Detainers with Optical Devices 499

Radiographic Techniques 499
Analyzing Change Keys to Reverse-Engineer the System 499
Top-Level Master Key Extrapolation 500
Extrapolation, Defined 501
The Security Threat 501
Practical Considerations, Variables, and Tactics 501
Information and Intelligence Before an Extrapolation Attempt 503
Decoding Options and Logistics 505
Decoding the top-level master key with a Change Key in One Session 505
Decoding the top-level master key with a Change Key in Multiple Sessions 505
Decoding the top-level master key with All Possible Permutations Precut in One or More Sessions 505

Chapter 22 Advanced Attacks on Key Control: 3D Printers and Special Software 507
3D Printing vs. EasyEntrie Milling Machines 510
3D Printer Technology 511
Fused Deposition Modeling Technology 511
Stereolithography Technology 512
Selective Laser Sintering Technology 514
Wax Casting 514
Specialized 3D Software for Keys 514
An Overview of Typical Program Capabilities 515

Chapter 23 Digital Fingerprints of Locks: Electronic Decoding Systems 523
Scanner Tools, Technology, and Physics 524
Primary Patents 526
A Common Transducer 526
Transducer Assembly 527
Reference Software 527
Scanner Designs: Current State-of-the-Art 527
M-SCAN Ultrasonic Lock Decoder and Sound Wave Decoder (SWD Version 4): An Overview 528
The Process of Scanning a Lock 531
Scanner Capabilities: A Summary of Required Features 532
Visualization of Scans 533

Chapter 24 Code-Setting Keys: A Case Study of an Attack on High-Security Key Control 537
Background Facts and the Initial Problem 538
An Overview of the Medeco Design 539
Could We Bump Open a Medeco Lock? 540
The Premise That Medeco Locks Could Not Be Bumped Open 541
The Premise That Medeco Locks Could Be Bumped Open 542
Lessons Learned 544

Part VI Specific Case Examples 545

Chapter 25 Case Examples from Part VII Rules 547
The Introduction of Focused Energy Against Internal Locking Components 549
A Paper Clip Defeats a Clever Security Enhancement 550
Defeat of Electronic Credentials 551
Defeat of an Electronic Access Control Lock Remote Using a Pin 553
Defeat of the Most Popular Vehicle Anti-Theft Device with a Shim Wire 553
The Hundred-Million-Dollar Diamond Heist 555
Vulnerable Design of an Electromechanical Door Lock, and the Murder of Three People 557
Absence of Evidence of Entry Doesn't Mean a Lock Wasn't Opened 559
Unknown Tools Specified in Standards Can Produce Invalid Results 559
Any Opening in a Lock Body or Accessible Component Can Provide a Manipulation Path 560
Attacks Against Integrated Circuits, Causing Them to Become Unstable 560
Simple Attacks Against Sophisticated, High-Security, or Complex Locks May Be All That's Required 560
The Most Popular Bike Lock in the World Opened by a Ballpoint Pen 561
Axial Locks: Targets for Easy Opening by Bumping and Impressioning 562
Experts Think High-Security Locks Can't Be Bumped Open 562
Multiple Security Layers Don't Make a Lock Secure 563
A Key Isn't Ever What Unlocks a Lock 563
Attacks on Power Sources Can Affect Electronic Circuits and Cause Locks to Open 564
Arrogance and a Lack of Imagination Never Works 564
Small or Uncomplicated Design Changes Can Create New Security Challenges 565
A 25-Year-Old Embedded Design Defect 565
Man-in-the-Middle Attacks Can Allow Your Expensive Car to Be Stolen 566
Hidden or Unknown Security or Design Information About a Device Doesn't Make It Secure 567
The Most Likely Attack Against an Electronic Lock May Not Be the Most Serious 568

Chapter 26 Case Examples By Category 571
Failure to Connect the Dots and Lack of Knowledge About Locks 572
Failure of Imagination and Engineering Incompetence 574

Failure to Consider or Deal with Hardware Constraints or Material Limitations 576
Failure to Understand or Correlate Attack Methods 577
Failure to Consider the Application of Force 578
Failure to Consider Decoding Methods and Attacks 582
Complex Attacks and Security Failures in Designs 586
Attacks on Lock Bodies and Integrity 588
Attacks on Credentials 591
Attacks on Electronic Elements 592
Attacks on Internal Locking Components 593
Attacks on Openings with Shims and Wires 594
Shear Line Attacks 595

Part VII Design Rules, Axioms, and Principles 597

Chapter 27 Design Rules, Axioms, and Guidelines 599

Epilogue 625

Appendix A Patents Issued 627

Appendix B Trademark Listing 629

Index 633

Tobias828259_ftoc.indd 32 1/8/2024 2:35:20 PM

Foreword

The delicate art of security engineering, at its core, is a balancing act. On one side rests the ever-evolving spectrum of innovation: the creation of locks that safeguard our most cherished assets. On the other is the constant challenge to compromise these very inventions—a process as old as time that Marc Weber Tobias insightfully delves into within the pages of this book.

Having served for 19 years as the CTO of dormakaba, one of the world's largest lock manufacturers, I have been at the intersection of innovation and vulnerability. Often, avoidable flaws surfaced, ushering in labor-intensive reparations and tarnishing a reputation painstakingly built over the years. This urgent reminder has always been that in the world of security, there is no room for complacency. From a corporate standpoint, a security failure isn't just a product glitch: it's a liability. The reverberations of such failures can be far-reaching, ranging from reputational harm to potential lawsuits.

Security, I believe, goes beyond mere functionality. It's a philosophy that embraces an understanding of systems and recognizes the complexities woven into the fabric of interconnected technology. Today's digital era intensifies this complexity, urging industry leaders to not just focus on how a system *works* but also understand the myriad ways it can be exploited. This dual vision is vital. At dormakaba, I've tried to instill this approach, advocating for both creators and challengers to scrutinize our products before they reach our customers.

Marc and I have collaborated for over a decade. We've confronted multiple designs, revealing vulnerabilities that escaped our initial engineering discernment. This iterative process, while humbling, has been an indispensable exercise. It has reaffirmed a belief I've always held that security isn't just a technical endeavor but an attitude—an attitude that demands humility, continuous learning, and a touch of paranoia.

Tobias828259_flast.indd 33 1/2/2024 7:06:28 PM

As Marc elucidates in this book, an industry-wide disconnect exists: engineers are well equipped with the skills to conceive and implement, but the art of understanding bypass techniques, both elementary and advanced, often remains uncharted. Standards aren't sufficient, as they frequently don't contemplate combining more than one technique to defeat sophisticated systems. This underestimation and lack of imagination of how to compromise supposed security poses significant threats, not just in terms of physical security but also in the realms of reputation and customer trust.

It's an unsettling revelation and one that Marc highlights with meticulous detail. Through an in-depth exploration from the history of lock designs to the nuances of modern-day lock vulnerabilities, this book bridges the gap between proven wisdom and contemporary challenges. For design engineers, risk managers, and even company executives, it provides the guidance and knowledge missing in traditional curricula to tackle real-world security issues.

It's not just a guide but a clarion call to an industry. It's a call to reevaluate, learn, and constantly challenge our understanding of security. I earnestly believe that this book isn't just "good to read" but is a necessary manual for anyone in the realm of security engineering and management.

As our world becomes more connected, the stakes get higher. The chain of security becomes ever more complex and intricate, emphasizing the need for a holistic approach to security engineering.

For the engineers and decision-makers of tomorrow, this book might just be their indispensable compass that points toward a more secure future.

—Andreas Martin Haeberli, Ph.D.

Former CTO, dormakaba

Introduction

Locks and keys, in various forms, have been employed to protect people, places, information, and assets for the past 4,000 years. Although they may outwardly appear simple, their design can be incredibly complex if they're to work properly and securely.

I have been deeply involved in the analysis and design of locks for 40 years and hold many patents on their bypass. Within the last 20 years, the industry has experienced a lock design revolution, partly due to the integration of microprocessors and sophisticated software, especially for access control applications. Improvements in metallurgy, combined with new manufacturing technology, have allowed the development of locks that can better resist criminal attacks. Modern techniques can produce locks with tolerances as high as .002″ and complex designs, yet with all the advances, security is often at risk. Why?

Unfortunately, the industry is still plagued by a fundamental problem in designing locks that must resist ever-developing new vulnerabilities and attacks. That problem partly results from how mechanical engineers are educated in engineering curriculums at universities. Typically, they're taught design theory and *how to make things work*. They aren't taught how to compromise or break their designs or possess the requisite knowledge for "insecurity engineering." This problem has become vastly more complicated by the introduction, integration, and overlay of software-based locking elements, working either alone or in concert with traditional mechanical components.

Electromechanical and electronic locks are slowly changing the landscape in physical security, but they're subject to even more attacks by "lock pickers" and hackers. Technologies such as 3D printing, radio frequency (RF) and electromagnetic pulse (EMP) generators, electronic and mechanical decoders,

Tobias828259_fintro.indd 35 1/2/2024 7:06:23 PM

and various forms of lock bumping, along with the employment of more sophisticated attack vectors, raise the stakes for manufacturers and end users. These problems pervade the industry and highlight the inability of engineers to think "out of the box" to conceive of possible methods of compromise or failure.

Manufacturers' loss of engineering talent through retirement or budget cutbacks has also exacerbated the problem and elevated the urgency of lock security. The loss of seasoned design engineers has largely erased the institutional memory of prior design failures.

What Does This Book Cover?

In the simplest of terms, this book is about what makes a lock or associated hardware "secure" and what can go wrong in the design. In more than one case, the result was the expenditure of millions of dollars on the research and development (R&D) of a high-security lock that was defeated in a few seconds by an 11-year-old kid with virtually no expertise. In my experience consulting for most of the world's largest lock manufacturers, lock designs fail because of a *lack of imagination* on the part of everyone involved in the process. This lack of imagination has had significant and costly ramifications in terms of security failures, legal damages, an inability to meet state and federal standards, and a loss of credibility among customers. Ultimately, it puts consumers at risk, and they usually don't know it. The results are from what I call *insecurity engineering*, which is the inability to design secure locks because of many factors in the education and training of engineers. That is what this book is about.

I started "breaking" things at the age of five years and made a career of discovering and exploiting security and related legal vulnerabilities in locks, safes, and security systems. The locks business is complex, involving liability and compliance issues and engineering requirements. *Tobias on Locks and Insecurity Engineering* analyzes basic lock designs and presents examples of often-catastrophic design failures that sometimes resulted in death and property destruction, compromise of critical information, and millions of dollars in damages.

Who Should Read This Book

Tobias on Locks and Insecurity Engineering is written for design engineers, security and IT professionals, risk managers, government services, law enforcement and intelligence agencies, crime labs, criminal investigators, lawyers, and investigative locksmiths. Even among these professionals, there is a lack of understanding of how to evaluate locks regarding specific security requirements. Relying on

industry standards promulgated by Underwriters Laboratories and the Builders Hardware Manufacturers Association (and equivalent organizations overseas) does little to define what *security* means and how to defeat it when considering forced entry, covert entry, and key control issues.

The reader can expect to gain an in-depth insight into lock designs and technology and how to better assess whether specific solutions will meet security requirements for their needs. Detailed information is presented that can help prevent manufacturers from producing insecure locks and assist risk management personnel in reviewing current or proposed systems. For risk management, criminal investigators, and crime laboratories, the information provides a road map showing how locks and security systems can be or may have been compromised by criminals or rogue employees.

Conventions Used in This Book

This book uses certain typographic styles to help you quickly identify important information. In particular, be on the lookout for *italicized text*, which indicates key terms described at length for the first time in a chapter. (Italics are also used for emphasis.)

In addition to these text conventions, you will find the following conventions that highlight segments of text:

NOTE **A note indicates information that's useful or interesting, but that's somewhat peripheral to the main text.**

TIP **A tip provides information that can save you time or frustration and that may not be entirely obvious.**

WARNING **Warnings describe potential pitfalls or the danger of failing to heed a warning.**

SIDEBARS

A sidebar is like a note but longer. The information in a sidebar is useful, but it doesn't fit into the main flow of the text.

Additional Resources

For additional information about locks, please check out the following resources:

- `https://Securitylaboratories.org`

- https://lss-dame.com for detailed videos of the compromise of locks and safes
- https://zieh-fix.com for the latest in bypass tools
- Roger G. Johnston, Ph.D., security expert, author of several books on the subject, and editor of the *Journal of Physical Security:* www.linkedin.com/in/rogergjohnston
- *High-Security Mechanical Locks: An Encyclopedic Reference*, 2007, by Graham Pulford

For additional information about the leading innovators in the lock-manufacturing industry, please check out the following resources:

- Abloy, Finland: www.abloy.com/global/en
- Allegion, Ireland and United States: https://us.allegion.com/en/index.html
- ASSA ABLOY, Sweden: https://assaabloy.com/group/en
- dormakaba, Germany: https://dormakaba.com/us-en
- EVVA, Austria: https://evva.com/int-en
- Ikon, Germany: https://ikon.de/de/en
- iLOQ, Finland: https://iloq.com/en
- Kensington Technology Group, United States: https://kensington.com
- Kwikset, United States: https://kwikset.com
- Medeco, United States: https://medeco.com/en
- Mul-T-Lock, Israel: https://mul-T-lock.com/global/en/about/mul-T-lock-international
- SaltoSystems, Spain: https://saltosystems.com/en
- Schlage, United States: https://schlage.com/en/home.html
- Videx, United States: https://videx.com

Finally, the multimedia edition of this book contains extensive video segments and graphics that demonstrate different attack vectors to compromise locks and safes that are referred to in this book. You can find this information at https://securitylaboratories.org and www.wiley.com/go/tobiasonlocks.

How to Contact the Author

I would appreciate your input, questions, feedback, and information on new tools and bypass techniques! You can find me on Skype, LinkedIn, WhatsApp, Telegram, and Signal. My website is https://securitylaboratories.org, and

you can email me at mwtobias@securitylaboratories.org or send secure email at mwtobias@protonmail.com.

How to Contact the Publisher

If you believe you've found a mistake in this book, please bring it to our attention by emailing our reader support team at wileysupport@wiley.com with the subject line "Possible Book Errata Submission."