

Table of contents

Introduction xxv

Who This Book is For xxvii

What is Covered in This Book? xxvii

MFA is Good xxx

How to Contact Wiley or the Author xxxi

Part I Introduction 1

1 Logon Problems 3

It's Bad Out There 3

The Problem with Passwords 5

Password Basics 9

Identity 9

The Password 10

Password Registration 11

Password Complexity 11

Password Storage 12

Password Authentication 13

Password Policies 15

Passwords Will Be with Us for a While 18

Password Problems and Attacks 18

Password Guessing 19

Password Hash Cracking 23

Password Stealing 27

Passwords in Plain View 28

Just Ask for It 29

Password Hacking Defenses 30

MFA Riding to the Rescue? 31

Summary 32

2 Authentication Basics 33

Authentication Life Cycle 34

Identity 35

Authentication 46

Authorization 54

Accounting/Auditing 54

Standards 56

Laws of Identity 56

Authentication Problems in the Real World 57

Summary 58

3 Types of Authentication 59

Personal Recognition 59

Knowledge-Based Authentication 60

Passwords 60

PINS 62

Solving Puzzles 64

Password Managers 69

Single Sign-Ons and Proxies 71

Cryptography 72

Encryption 73

Public Key Infrastructure 76

Hashing 79

Hardware Tokens 81

One-Time Password Devices 81

Physical Connection Devices 83

Wireless 87

Phone-Based 89

Voice Authentication 89

Phone Apps 89

SMS 92

Biometrics 92

FIDO 93

Federated Identities and APIs 94

OAuth 94

APIs 96

Contextual/Adaptive 96

Less Popular Methods 97

Voiceover Radio 97

Paper-Based 98

Summary 99

4 Usability vs Security 101

What Does Usability Mean?	101
We Don't Really Want the Best Security	103
Security Isn't Usually Binary	105
Too Secure	106
Seven-Factor MFA	106
Moving ATM Keypad Numbers	108
Not as Worried as You Think About Hacking	109
Unhackable Fallacy	110
Unbreakable Oracle	113
DJB	113
Unhackable Quantum Cryptography	114
We are Reactive Sheep	115
Security Theater	116
Security by Obscurity	117
MFA Will Cause Slowdowns	117
MFA Will Cause Downtime	118
No MFA Solution Works Everywhere	118
Summary	119
Part II Hacking MFA	121
5 Hacking MFA in General	123
MFA Dependency Components	124
Enrollment	125
User	127

Devices/Hardware 127

Software 128

API 129

Authentication Factors 129

Authentication Secrets Store 129

Cryptography 130

Technology 130

Transmission/Network Channel 131

Namespace 131

Supporting Infrastructure 131

Relying Party 132

Federation/Proxies 132

Alternate Authentication Methods/Recovery 132

Migrations 133

Deprovision 133

MFA Component Conclusion 134

Main Hacking Methods 134

Technical Attacks 134

Human Element 135

Physical 137

Two or More Hacking Methods Used 137

“You Didn’t Hack the MFA!” 137

How MFA Vulnerabilities are Found 138

Threat Modeling 138

Code Review 138

Fuzz Testing 138

Penetration Testing 139

Vulnerability Scanning 139

Human Testing 139

Accidents 140

Summary 140

6 Access Control Token Tricks 141

Access Token Basics 141

Access Control Token General Hacks 142

Token Reproduction/Guessing 142

Token Theft 145

Reproducing Token Hack Examples 146

Network Session Hijacking Techniques and Examples 149

Firesheep 149

MitM Attacks 150

Access Control Token Attack Defenses 157

Generate Random, Unguessable Session IDs 157

Use Industry-Accepted Cryptography and Key Sizes 158

Developers Should Follow Secure Coding Practices 159

Use Secure Transmission Channels 159

Include Timeout Protections 159

Tie the Token to Specific Devices or Sites 159

Summary 161

7 Endpoint Attacks 163

Endpoint Attack Risks 163

General Endpoint Attacks 165

Programming Attacks 165

Physical Access Attacks 165

What Can an Endpoint Attacker Do? 166

Specific Endpoint Attack Examples 169

Bancos Trojans 169

Transaction Attacks 171

Mobile Attacks 172

Compromised MFA Keys 173

Endpoint Attack Defenses 174

MFA Developer Defenses 174

End-User Defenses 177

Summary 179

8 SMS Attacks 181

Introduction to SMS 181

SS7 184

Biggest SMS Weaknesses 186

Example SMS Attacks 187

SIM Swap Attacks 187

SMS Impersonation	191
SMS Buffer Overflow	194
Cell Phone User Account Hijacking	195
Attacks Against the Underlying Supporting Infrastructure	196
Other SMS-Based Attacks	196
SIM/SMS Attack Method Summary	197
NIST Digital Identity Guidelines Warning	198
Defenses to SMS-Based MFA Attacks	199
Developer Defenses	199
User Defenses	201
Is RCS Here to Save Mobile Messaging?	202
Is SMS-Based MFA Still Better than Passwords?	202
Summary	203
9 One-Time Password Attacks	205
Introduction to OTP	205
Seed Value-Based OTPs	208
HMAC-Based OTP	209
Event-Based OTP	211
TOTP	212
Example OTP Attacks	217
Phishing OTP Codes	217
Poor OTP Creation	219
OTP Theft, Re-Creation, and Reuse	219

Stolen Seed Database 220

Defenses to OTP Attacks 222

Developer Defenses 222

Use Reliable and Trusted and Tested OTP Algorithms 223

OTP Setup Code Must Expire 223

OTP Result Code Must Expire 223

Prevent OTP Replay 224

Make Sure Your RNG is NIST-Certified or Quantum 224

Increase Security by Requiring Additional Entry Beyond OTP Code 224

Stop Brute-Forcing Attacks 224

Secure Seed Value Database 225

User Defenses 225

Summary 226

10 Subject Hijack Attacks 227

Introduction 227

Example Attacks 228

Active Directory and Smartcards 228

Simulated Demo Environment 231

Subject Hijack Demo Attack 234

The Broader Issue 240

Dynamic Access Control Example 240

ADFS MFA Bypass 241

Defenses to Component Attacks 242

Threat Model Dependency Abuse Scenarios 242

Secure Critical Dependencies 242

Educate About Dependency Abuses 243

Prevent One to Many Mappings 244

Monitor Critical Dependencies 244

Summary 244

11 Fake Authentication Attacks 245

Learning About Fake Authentication Through UAC 245

Example Fake Authentication Attacks 251

Look-Alike Websites 251

Fake Office 365 Logons 252

Using an MFA-Incompatible Service or Protocol 253

Defenses to Fake Authentication Attacks 254

Developer Defenses 254

User Defenses 256

Summary 257

12 Social Engineering Attacks 259

Introduction 259

Social Engineering Commonalities 261

Unauthenticated Communication 261

Nonphysical 262

Usually Involves Well-Known Brands 263

Often Based on Notable Current Events and Interests 264

Uses Stressors 264

Advanced: Pretexting 265

Third-Party Reliances 266

Example Social Engineering Attacks on MFA 266

Fake Bank Alert 267

Crying Babies 267

Hacking Building Access Cards 268

Defenses to Social Engineering Attacks on MFA 270

Developer Defenses to MFA 270

User Defenses to Social Engineering Attacks 271

Summary 273

13 Downgrade/Recovery Attacks 275

Introduction 275

Example Downgrade/Recovery Attacks 276

Alternate Email Address Recovery 276

Abusing Master Codes 280

Guessing Personal-Knowledge Questions 281

Defenses to Downgrade/Recovery Attacks 287

Developer Defenses to Downgrade/Recovery Attacks 287

User Defenses to Downgrade/Recovery Attacks 292

Summary 294

14 Brute-Force Attacks 295

Introduction 295

Birthday Attack Method	296
Brute-Force Attack Methods	297
Example of Brute-Force Attacks	298
OTP Bypass Brute-Force Test	298
Instagram MFA Brute-Force	299
Slack MFA Brute-Force Bypass	299
UAA MFA Brute-Force Bug	300
Grab Android MFA Brute-Force	300
Unlimited Biometric Brute-Forcing	300
Defenses Against Brute-Force Attacks	301
Developer Defenses Against Brute-Force Attacks	301
User Defenses Against Brute-Force Attacks	305
Summary	306
15 Buggy Software	307
Introduction	307
Common Types of Vulnerabilities	308
Vulnerability Outcomes	316
Examples of Vulnerability Attacks	317
Uber MFA Vulnerability	317
Google Authenticator Vulnerability	318
YubiKey Vulnerability	318
Multiple RSA Vulnerabilities	318
SafeNet Vulnerability	319

Login gov 319

ROCA Vulnerability 320

Defenses to Vulnerability Attacks 321

Developer Defenses Against Vulnerability Attacks 321

User Defenses Against Vulnerability Attacks 322

Summary 323

16 Attacks Against Biometrics 325

Introduction 325

Biometrics 326

Common Biometric Authentication Factors 327

How Biometrics Work 337

Problems with Biometric Authentication 339

High False Error Rates 340

Privacy Issues 344

Disease Transmission 345

Example Biometric Attacks 345

Fingerprint Attacks 345

Hand Vein Attack 348

Eye Biometric Spoof Attacks 348

Facial Recognition Attacks 349

Defenses Against Biometric Attacks 352

Developer Defenses Against Biometric Attacks 352

User/Admin Defenses Against Biometric Attacks 354

Summary 355

17 Physical Attacks 357

Introduction 357

Types of Physical Attacks 357

Example Physical Attacks 362

Smartcard Side-Channel Attack 362

Electron Microscope Attack 364

Cold-Boot Attacks 365

Snooping On RFID-Enabled Credit Cards 367

EMV Credit Card Tricks 370

Defenses Against Physical Attacks 370

Developer Defenses Against Physical Attacks 371

User Defenses Against Physical Attacks 372

Summary 375

18 DNS Hijacking 377

Introduction 377

DNS 378

DNS Record Types 382

Common DNS Hacks 382

Example Namespace Hijacking Attacks 388

DNS Hijacking Attacks 388

MX Record Hijacks 388

Dangling CDN Hijack 389

Registrar Takeover 390

DNS Character Set Tricks 390

ASN 1 Tricks 392

BGP Hijacks 392

Defenses Against Namespace Hijacking Attacks 393

Developer Defenses 394

User Defenses 395

Summary 397

19 API Abuses 399

Introduction 399

Common Authentication Standards and Protocols Involving APIs 402

Other Common API Standards and Components 411

Examples of API Abuse 414

Compromised API Keys 414

Bypassing PayPal 2FA Using an API 415

AuthO MFA Bypass 416

Authy API Format Injection 417

Duo API As-Designed MFA Bypass 417

Microsoft OAuth Attack 419

Sign In with Apple MFA Bypass 419

Token TOTP BLOB Future Attack 420

Defenses Against API Abuses 420

Developer Defenses Against API Abuses 420

User Defenses Against API Abuses 422

Summary 423

20 Miscellaneous MFA Hacks 425

Amazon Mystery Device MFA Bypass 425

Obtaining Old Phone Numbers 426

Auto-Logon MFA Bypass 427

Password Reset MFA Bypass 427

Hidden Cameras 427

Keyboard Acoustic Eavesdropping 428

Password Hints 428

HP MFA DoS 429

Trojan TOTP 429

Hackers Turn MFA to Defeat You 430

Summary 430

21 Test: Can You Spot the Vulnerabilities? 431

Threat Modeling MFA Solutions 431

Document and Diagram the Components 432

Brainstorm Potential Attacks 432

Estimate Risk and Potential Losses 434

Create and Test Mitigations 436

Do Security Reviews 436

Introducing the Bloomberg MFA Device 436

Bloomberg, L P and the Bloomberg Terminal 437

New User B-Unit Registration and Use 438

Threat-Modeling the Bloomberg MFA Device 439

Threat-Modeling the B-Unit in a General Example 440

Specific Possible Attacks 441

Multi-Factor Authentication Security Assessment Tool 450

Summary 451

Part III Looking Forward 453

22 Designing a Secure Solution 455

Introduction 455

Exercise: Secure Remote Online Electronic Voting 457

Use Case Scenario 457

Threat Modeling 458

SDL Design 460

Physical Design and Defenses 461

Cryptography 462

Provisioning/Registration 463

Authentication and Operations 464

Verifiable/Auditable Vote 466

Communications 467

Backend Blockchain Ledger 467

Migration and Deprovisioning 470

API 470

Operational Training 470

Security Awareness Training 470

Miscellaneous 471

Summary 471

23 Selecting the Right MFA Solution 473

Introduction 473

The Process for Selecting the Right MFA Solution 476

Create a Project Team 477

Create a Project Plan 478

Educate 479

Determine What Needs to Be Protected 479

Choose Required and Desired Features 480

Research/Select Vendor Solutions 488

Conduct a Pilot Project 490

Select a Winner 491

Deploy to Production 491

Summary 491

24 The Future of Authentication 493

Cyber Crime is Here to Stay 493

Future Attacks 494

Increasing Sophisticated Automation 495

Increased Nation-State Attacks 496

Cloud-Based Threats 497

Automated Attacks Against MFA 497

What is Likely Staying 498

Passwords 498

Proactive Alerts 498

Preregistration of Sites and Devices 499

Phones as MFA Devices 500

Wireless 501

Changing/Morphing Standards 501

The Future 501

Zero Trust 502

Continuous, Adaptive, Risk-Based 503

Quantum-Resistant Cryptography 506

Interesting Newer Authentication Ideas 506

Summary 507

25 Takeaway Lessons 509

Broader Lessons 509

MFA Works 509

MFA is Not Unhackable 510

Education is Key 510

Security Isn't Everything 511

Every MFA Solution Has Trade-Offs 511

Authentication Does Not Exist in a Vacuum 512

There is No Single Best MFA Solution for Everyone 515

There are Better MFA Solutions 515

MFA Defensive Recap 516

Developer Defense Summary 516

User Defense Summary 518

Appendix: List of MFA Vendors 521