

# CONTENTS

## PREFACE

What This Book Is About	xvii
Who This Book Is For	xviii
Acknowledgments	xix

## CHAPTER 1 THE AUTHENTICATION LANDSCAPE

1.1	A Very Old Story	1
1.2	Elements of an Authentication System	3
	Revised Attacks and Revised Defenses	
	Security Strategies	
1.3	Authentication in Timesharing Systems	10
	Passwords Under Attack	
	Hashed Passwords	
1.4	Attacking the Secret	17
	Guessing Attacks	
	Social Engineering	
1.5	Sniffing Attacks	23
	Sniffing in Software	
	Trojan Login	
	Van Eck Sniffing	
1.6	Authentication Factors	28
1.7	Judging Attack Prevalence	32
1.8	Summary Tables	34

## CHAPTER 2 EVOLUTION OF REUSABLE PASSWORDS

2.1	Passwords: Something You Know	39
2.2	Authentication and Base Secrets	43
	Cultural Authentication	
	Random Secrets	
2.3	The Unix Password System	47

2.4	Attacking the Unix Password File	51
	The M-209 Hash	
	The DES Hash	
2.5	Dictionary Attacks	56
2.6	The Internet Worm	58
2.7	Resisting Guessing Attacks	63
	Randomness and Bit Spaces	
	Biases in Base Secrets	
	Average Attack Space	
2.8	Summary Tables	69

### CHAPTER 3 INTEGRATING PEOPLE

3.1	Roles People Play	73
	Insiders and Outsiders	
	Users and Administrators	
	Carriers and Crackers	
3.2	Enrolling Users	80
	Self-Authentication	
	Enrollment in Person	
3.3	Assigning an Initial Secret	83
	Random Secret	
	Cultural Secret	
	Changing the Initial Password	
3.4	Entropy and User Password Selection	87
	Statistical Bias in Text	
	Dictionary Attacks	
	Estimating Bias in Password Selection	
3.5	Restricting Password Selection	94
	Therapeutic Password Cracking	
	Automatic Password Generation	
	Proactive Password Checking	
	Limitations on Password Strength	
3.6	Summary Tables	100

## CHAPTER 4 DESIGN PATTERNS

4.1	Patterns in Authentication Systems	103
4.2	The Role of Physical Security	105
	Protecting Software Authentication	
	Protecting Workstations	
	Hardware Protection of Authentication	
4.3	Administrative Requirements	113
	Physical Protection	
	Ease of Authentication	
	Efficient Administration	
4.4	Local Authentication	118
4.5	Direct Authentication	120
4.6	Indirect Authentication	122
	Authentication Protocols	
	Indirect Authentication Protocols	
4.7	Off-Line Authentication	125
4.8	Applying the Patterns	128
4.9	Summary Tables	130

## CHAPTER 5 LOCAL AUTHENTICATION

5.1	Laptops and Workstations	133
5.2	Workstation Encryption	136
	File Encryption	
	Volume Encryption	
5.3	Encryption for Data Protection	143
	Shortcut Attacks on Encryption	
	Trial-and-Error Attacks on Encryption	
	Theoretical Guess-Rate Limitations	
5.4	Key-Handling Issues	149
	Memorized Keys	
	Key-Handling Policies	
	Key Escrow and Crypto Politics	
5.5	Summary Tables	153

**CHAPTER 6**  
**PICKING PINS AND PASSWORDS**

6.1	Password Complexity	155
	Passwords and Usability	
	Forcing Functions and Mouse Pads	
6.2	Different Secrets for Different Uses	163
	Sniffable Passwords	
	PIN Applications	
	Internal Passwords	
	External Passwords	
6.3	Improving Internal Password Entry	169
	Operator-Controlled Password Display	
	Report Incorrect User Names	
	Allow Many Password Guesses	
	Report Incorrect Password Attempts	
	Avoid Periodic Password Changes	
6.4	Password Selection	174
	Internal Passwords	
	External and Administrative Passwords	
6.5	Shared Passwords	178
	Multiple-Use Passwords	
	Password Delegation	
6.6	Storing Written Passwords	181
	Physical Custody	
	Locked Storage	
	Electronic Storage	
6.7	Sequences and Groups of Passwords	188
	Password Sequences	
	Forward Secrecy With Theme Words	
	Passwords From Songs and Poems	
6.8	Summary Tables	192

## CHAPTER 7 BIOMETRICS

7.1	Biometrics: Something You Are Promise and Reality Uses of Biometrics	193
7.2	Biometric Techniques Measuring Physical Traits Measuring Behavioral Traits	198
7.3	How Biometrics Work	203
7.4	Taking a Biometric Reading Feedback During Biometric Input Forging a Physical Trait	205
7.5	Building and Matching Patterns Example: A Trivial Hand Geometry Biometric Enrolling a User	208
7.6	Biometric Accuracy Trading Off Usability and Security Average Attack Space	211
7.7	Biometric Encryption Preserving Secrecy Authenticity of Biometric Data The Problem of Biometric Exploitation	216
7.8	Summary Tables	220

## CHAPTER 8 AUTHENTICATION BY ADDRESS

8.1	Who Versus Where	223
8.2	Telephone Numbers as Addresses Identification via Dial-Back Dial-Up Identification: Caller ID	225
8.3	Network Addresses Addressing on the ARPANET Internet Protocol Addresses	230
8.4	Attacks on Internet Addresses IP Address Theft Denial of Service Attacks	234
8.5	Effective Source Authentication	240

8.6	Unix Local Network Authentication	242
	The “r” Commands	
	Remote Procedure Calls, NFS, and NIS	
8.7	Authenticating a Geographical Location	248
8.8	Summary Tables	251

## CHAPTER 9 AUTHENTICATION TOKENS

9.1	Tokens: Something You Have	255
	Passive Tokens	
	Active Tokens	
9.2	Network Password Sniffing	261
9.3	One-Time Passwords	264
	Counter-Based One-Time Passwords	
	Clock-Based One-Time Passwords	
9.4	Attacks on One-Time Passwords	271
	Man in the Middle Attack	
	IP Hijacking	
9.5	Incorporating a PIN	273
	PIN Appended to an External Password	
	PIN as an Internal Password	
	PIN as Part of the Base Secret	
9.6	Enrolling Users	278
9.7	Summary Tables	282

## CHAPTER 10 CHALLENGE RESPONSE PASSWORDS

10.1	Challenge Response	285
	Challenge Response and X9.9	
	S/Key Authentication	
10.2	Challenge Response Issues	292
	User Interaction	
	Known Ciphertext Attack on ANSI X9.9	
10.3	Password Token Deployment	294
	Soft Tokens	
	Handling Multiple Servers	
	Proprietary Implementations	

10.4	Evolving Windows Authentication	298
	LANMAN Hashing	
	Attacking the LANMAN Hash	
	Plaintext Passwords on Windows	
10.5	Windows Challenge Response	304
	Attacking Windows Challenge Response	
10.6	Windows NTLM Authentication	306
	Attacking the NT Password Database	
	Attacking NTLM Challenge Response	
10.7	Summary Tables	311

## **CHAPTER 11**

### **INDIRECT AUTHENTICATION**

11.1	Indirect Authentication	313
	Network Boundary Control	
	One-Time Password Products	
	LAN Resource Control	
11.2	RADIUS Protocol	318
	A RADIUS Logon	
	Protecting RADIUS Messages	
	RADIUS Challenge Response	
11.3	Encrypted Connections and Windows NT	325
	Encrypted Connections	
	Integrity Protection	
	Politics, Encryption, and Technical Choices	
11.4	Windows NT Secure Channels	332
	Secure Channel Keying	
	Attacks on Secure Channels	
11.5	Computers' Authentication Secrets	336
11.6	Summary Tables	338

**CHAPTER 12**  
**KERBEROS AND WINDOWS 2000**

12.1	The Key Distribution Center	341
	Tickets	
	Needham-Schroeder	
12.2	Kerberos	348
	The Authentication Server	
	Authenticating to a Server	
	Ticket-Granting Service	
12.3	User and Workstation Authentication	355
	Workstation Authentication	
	Preauthentication	
12.4	Ticket Delegation	357
	Proxiable TGT	
	Forwardable TGT	
	Realms and Referral Tickets	
12.5	Attacking a Kerberos Network	361
	Intrusion Tolerance	
	Clock Synchronization	
12.6	Kerberos in Windows 2000	363
	Master Keys and Workstation Authentication	
	Service and Protocol Support	
12.7	Summary Tables	367

**CHAPTER 13**  
**PUBLIC KEYS AND**  
**OFF-LINE AUTHENTICATION**

13.1	Public Key Cryptography	369
13.2	The RSA Public Key Algorithm	373
13.3	Attacking RSA	375
	Attacking RSA Keys	
	Attacking Digital Signatures	
13.4	The Digital Signature Standard	380
13.5	Challenge Response Revisited	383
	LOCKOut Fortezza Authentication Protocol	
	FIPS 196 Authentication	

13.6	Secure Sockets Layer	389
	Establishing Keys with SSL	
	Authentication with Typical SSL	
	SSL Client Authentication	
13.7	Public Keys and Biometrics	397
13.8	Summary Tables	399

## **CHAPTER 14**

### **PUBLIC KEY**

### **CERTIFICATES**

14.1	Tying Names to Public Keys	401
	Certificate Authorities	
	Using the Right Certificate	
14.2	Creating Certificates	408
	Certificate Standards	
	Certificates and Access Control	
14.3	Certificate Authorities	412
	Proprietors as Certificate Authorities	
	Commercial Certificate Authorities	
14.4	Public Key Infrastructure	415
	Centralized Hierarchy	
	Authority Lists	
	Cross-Certification	
14.5	Personal Certification	420
	Certified by Reputation	
	Certified by a Web of Trust	
14.6	Certificate Revocation	423
	Certificate Revocation List	
	On-line Revocation	
	Timely Certification	
14.7	Certificates with Kerberos	426
14.8	Summary Tables	428

## **CHAPTER 15**

### **PRIVATE KEY SECURITY**

15.1	Generating Private Keys	431
15.2	The Private Key Storage Problem	433
15.3	Smart Cards and Private Keys	434
	Off-Card Key Generation	
	On-Card Key Generation	
15.4	Smart Card Access Control	438
	PINs	
	Biometrics	
15.5	Private Keys on Servers	442
	Novell NetWare: Key Downloading	
	Safeword Virtual Smart Card: Data Uploading	
15.6	Passwords Revisited	449
15.7	Summary Tables	450
	<b>Chapter Notes</b>	<b>451</b>
	<b>Bibliography</b>	<b>471</b>
	<b>Web and Vendor Resources</b>	<b>491</b>
	<b>Glossary</b>	<b>501</b>
	<b>Index</b>	<b>519</b>