# Contents

1 Authentication Basics ........ 1
Introduction ........ 2
Types of Authentication Approaches ........ 3
Type I: What You Know? ........ 3
Type II: What You Have? ........ 17
Type III: What You Are? ........ 21
Type IV: Where You Are? ........ 28
User Account Types ........ 29
Chapter Summary ........ 30
References ........ 35
2 Biometric Authentication ........ 37
Introduction ........ 38
Different Biometric Modalities ........ 40
Biometric Authentication Process ........ 42
Performance Measures of Biometric Systems ........ 45
False Acceptance Rate (FAR) ........ 45
False Rejection Rate (FRR) ........ 45
Equal Error Rate (EER) ........ 46
Failure to Enroll Rate (FTE) ........ 47
Failure to Acquire Rate (FTA) ........ 47
Details of Biometric Authentication Modalities ........ 47
Face Recognition ........ 47
Fingerprint Recognition ........ 49
Iris Recognition ........ 51
Retina Recognition ........ 52
Hand Geometry ........ 53
Voice (Speaker) Recognition ........ 55
Keystroke Recognition ........ 57
Gait-Based Recognition ........ 57
Brainprint ........ 61
Applications of Biometrics ........ 61
Banking ........ 63
Computer Access ........ 64
Immigration ........ 64
National Identity ........ 64
Prisons ........ 65
Telecommunications ........ 65
Time and Attendance ........ 65
Limitations of Biometric Systems ........ 66
New Biometric Challenges ........ 67
Attacks on Biometric-Based Authentication Systems ........ 69
Mitigating Different Attacks on Biometric Systems ........ 71
Liveness Detection Mechanisms ........ 71

Dasgupta, Dipankar
Advances in user authentication

digitalisiert durch:
IDS Basel Bern

Steganographic and Watermarking Techniques ..... 71
Challenge-Response Systems ..... 72
Multimodal Biometric Systems ..... 73
Soft Biometrics ..... 75
Cancelable Biometrics ..... 76
Comparative Evaluation ..... 77
Chapter Summary ..... 79
References ..... 82
3 Negative Authentication Systems ..... 85
Introduction ..... 86
Concept of Negative Authentication ..... 87
Types of NAS ..... 90
Implementation of Negative Authentication System (NAS) ..... 95
Chapter Summary ..... 143
References ..... 144
4 Pseudo-Passwords and Non-textual Approaches ..... 147
Evolution of Hash Functions ..... 148
Honeyword Approach ..... 149
Honeychecker ..... 150
**NLEs from the *n*-Gram Model Concept** ..... 156
NLEs from the PCFG Model Concept ..... 157
Encoding or Decoding of the Sub-grammar (SG) ..... 158
**Evaluating the Encoders** ..... 158
Evaluating Single Passwords ..... 159
**NoCrack Password Vaults** ..... 160
Bloom Filter ..... 161
**Constructing Bloom Filters** ..... 162
Comparison of Complementary Approaches: NAS (G-NAS, GM-NAS), Honeywords, and Bloom Filter ..... 164
Non-textual Passwords ..... 165
Recognition-Based Techniques ..... 167
Recall-Based Techniques ..... 171
Security Aspects and Possible Attacks on Graphical Passwords ..... 175
Chapter Summary ..... 179
References ..... 180
5 Multi-Factor Authentication ..... 185
Introduction ..... 186
Issues of Single-Factor Authentication (SFA) ..... 188
Two-Factor-Based Authentication ..... 188
Different Authentication Factors Considered in MFA ..... 190
Necessity to Move Toward MFA ..... 191
Different Characteristics of a Good MFA ..... 192
Easy to Use ..... 192
Scalable ..... 192
Resilient ..... 193
Reliable ..... 193

Single Sign-On........................................................ 193
Fast Identity Online (FIDO)........................................... 196
Universal Authentication Framework (UAF)............................ 198
Universal Second Factor (U2F)......................................... 198
How FIDO Works........................................................ 198
MFA Authentication Products......................................... 200
CA Strong Authentication ............................................ 201
Okta Verify.............................................................. 203
Vasco IDENTIKEY Authentication Server 3.8.......................... 205
Dell Defender........................................................... 206
Symantec Validation and ID Protection Service (VIP) ................. 210
RSA SECURID ........................................................... 213
SafeNet Authentication Service........................................ 215
SecureAuth IdP 8.0..................................................... 217
Microsoft Azure......................................................... 219
Swivel Secure........................................................... 221
DUO Security ........................................................... 222
Comparison of Various MFA Products ................................ 224
Chapter Summary ...................................................... 224
References.............................................................. 230
6 Continuous Authentication........................................... 235
Introduction............................................................ 236
Continuous/Active Authentication..................................... 236
Characteristics of a Good Continuous Authentication System............ 238
Steps to Design Continuous Authentication System..................... 239
Attribute Selection for Continuous Authentication System .............. 239
Unimodal Continuous Authentication.................................. 240
Face Recognition ...................................................... 240
Partial Face Recognition............................................... 241
Web Browsing Behavior................................................ 241
Dynamic Context Fingerprints......................................... 244
Keystroke Dynamics.................................................... 245
Cognitive Fingerprint .................................................. 246
Screen Fingerprints .................................................... 248
Stylistic Fingerprint .................................................... 250
Hand Movement, Orientation, and Grasp (HMOG) ...................... 251
Multi-modal Continuous Authentication ............................... 253
Keystroke and Mouse Movement, Application Usage,
and System Footprint.................................................. 253
Active Authentication for Mobile Devices ............................. 256
Stylometry, Application Usage, Web Browsing, and GPS Location......... 258
Multi-sensor Text-Based Biometric .................................... 259
Gestures, Keystroke, Touch, and Body Movements ...................... 261
Keystroke, Mouse Movement, Stylometry, Web Browsing Behavior........ 262
Smartphone-Based Multi-sensor Authentication........................ 263
Continuous Authentication for Internet of Things (IoT).................. 266

Self-authenticable Approaches for Wearable Devices .................... 267
The National Strategy for Trusted Identities in Cyberspace (NSTIC) ........ 269
Chapter Summary ................................................ 273
References ........................................................ 275
7 Adaptive Multi-factor Authentication ................................ 281
Introduction ...................................................... 282
Adaptive-MFA (A-MFA) Framework .................................... 283
Authentication Factor ............................................... 285
Considered Surrounding Conditions for MFA .......................... 285
Trustworthy Framework for Authentication Factors ..................... 288
First Approach .................................................... 288
Second Approach .................................................. 292
Adaptive Selection Approach for MFA ................................. 306
Implementation of Adaptive-MFA System .............................. 311
Surrounding Conditions (Light and Noise) ............................. 312
Database to Store Authentication Factors .............................. 313
Configuration of A-MFA System ....................................... 314
Client Application .................................................. 316
Experimental Results of the A-MFA System ............................ 336
Creation of Synthetic Dataset ......................................... 336
System Evaluation Criteria ............................................ 338
Experimental Results ................................................ 338
Comparison of Adaptive Selection Approach with Random
and Only Biometric-Based Approaches ................................. 342
Advantage over Other Existing MFA Approaches ......................... 345
Future Trends ....................................................... 347
Chapter Summary .................................................... 350
References .......................................................... 353
Service Part
Index ................................................................ 358