Inhaltsverzeichnis

Vorwort 13

1 Angriffe in Theorie und Praxis 19

1.1 „Angriffe" durch Forscher 19
1.2 Angriffe auf Schwachstellen... 25
1.2.1 ... bei Pwn2Own... 25
1.2.2 ... und Jailbreaking 27
1.3 Schadsoftware im Überblick 29
1.4 Bösartige Apps im App Store 31
1.5 Ein einziger wirklich schädlicher Angriff 34
1.6 Apple will keine Virenscanner 37
1.7 Fazit 37

2 Sicheres Booten, Sandbox & Co. – Die Schutzmaßnahmen im Überblick 39

2.1 Die sichere Boot-Kette 40
2.2 Signatur der Apps 43
2.3 Schutzmaßnahmen zur Laufzeit 44
2.4 Apps in der Sandbox 46
2.5 Rund um die Kryptografie 47
2.5.1 Der gerätespezifische Schlüssel 48
2.5.2 Die weiteren Schlüssel 50
2.5.3 Das Löschen von Schlüsseln 50
2.6 Schutz der Dateien 50

2.6.1 Data Protection im Überblick 51
2.6.2 Die Schutzklassen 52
2.6.3 Was kann geschützt werden? 55
2.7 Schutz der Daten im Schlüsselbund 55
2.8 Keybags 58
2.8.1 System Keybag 59
2.8.2 Backup Keybag 59
2.8.3 Escrow Keybag 60
2.8.4 iCloud Backup Keybag 61
2.8.5 Bestandteile eines Keybags 61
2.9 Netzwerksicherheit 62
2.9.1 SSL und TLS 62
2.9.2 VPN 63
2.9.3 Wi-Fi 64
2.9.4 Bluetooth 64
2.9.5 Keine Firewall 65
2.10 Sperrcode und Zugriffsschutz 66
2.10.1 Anforderungen an den Sperrcode 66
2.10.2 Touch ID – Fingerabdruck statt Sperrcode 68
2.10.3 Erzwingen einer bestimmten Konfiguration 70
2.10.4 Konfiguration der Geräte 71
2.10.5 Einschränkungen der Gerätefeatures 72
2.10.6 Konfigurationsprofile als Angriffsvektor 74
2.10.7 Löschen aus der Ferne (Remote Wipe) 75

3 Die Schutzmaßnahmen nutzen 77

3.1 Die sichere Boot-Kette 77
3.2 Signatur der Apps 78
3.3 Schutzmaßnahmen zur Laufzeit 79

3.3.1 Berechtigungen (Entitlements) 79
3.3.2 URL-Schemata 84
3.3.3 Das Erschweren von Pufferüberlauf-Exploits 85
3.4 Apps in der Sandbox 85
3.5 Rund um die Kryptografie 86
3.6 Schutz der Dateien 87
3.7 Schutz der Daten im Schlüsselbund 90
3.7.1 Die Daten im Schlüsselbund 90
3.7.2 Die Nutzung des Schlüsselbunds 92
3.8 Keybags 102
3.9 Netzwerksicherheit 102
3.9.1 SSL und TLS 102
3.9.2 VPN 114
3.9.3 Wi-Fi 114
3.9.4 Bluetooth 115
3.10 Sperrcode und Zugriffsschutz 115

4 Der Wegweiser zur sicheren Entwicklung 117

4.1 iOS ist nicht so sicher, wie Apple uns glauben macht! 117
4.2 Sichere App-Entwicklung 119
4.3 Der Weg ist das Ziel 119
4.4 Schwachstellen im Überblick 120
4.4.1 Objective-C ist auch nur C 120
4.4.2 Unzureichend geprüfte Eingaben 121
4.4.3 Interprozesskommunikation 122
4.4.4 Unsichere Dateioperationen 122
4.4.5 Schwachstellen in der Zugriffskontrolle, Authentifizierung und Autorisierung 123
4.4.6 Fehler in der Kryptografie 125

4.4.7 Race Conditions 125
4.4.8 Social Engineering 126
4.5 Die OWASP Top 10 Mobile Risks 127
4.5.1 M1: „Insecure Data Storage" 127
4.5.2 M2: „Weak Server Side Controls" 128
4.5.3 M3: „Insufficient Transport Layer Protection!" 129
4.5.4 M4: „Client Side Injection" 130
4.5.5 M5: „Poor Authorization and Authentication" 131
4.5.6 M6: „Improper Session Handling" 132
4.5.7 M7: „Security Decisions via untrusted Inputs" 132
4.5.8 M8: „Side Channel Data Leakage" 133
4.5.9 M9: „Broken Cryptography" 133
4.5.10 M10: „Sensitive Information Disclosure" 133

5 Ein sicherer Entwicklungszyklus 135

5.1 Der SDL im Überblick 136
5.1.1 Die Grundsätze des SDL 136
5.1.2 Die Phasen des SDL 138
5.1.3 Fazit 143
5.2 Bedrohungsmodelle – Application Threat Modeling 143
5.2.1 Bedrohungsmodelle im „Real Life" 143
5.2.2 Viele Wege führen zum Ziel 144
5.2.3 Entwurfsgesteuerte Bedrohungsmodellierung 145
5.2.4 STRIDE 147
5.2.5 Ein einfaches Beispiel 147

6 Pufferüberlauf- und Formatstring-Schwachstellen 151

6.1 Der Pufferüberlauf 151
6.1.1 Ein C-Programm und sein Speicher 152

6.1.2 Ein Pufferüberlauf auf dem Stack 153
6.1.3 Angriff über die Pufferüberlaufschwachstelle 155
6.1.4 Varianten des Pufferüberlaufs 156
6.1.5 Pufferüberläufe verhindern, allgemein 157
6.1.6 Schutzmaßnahmen erschweren Angriffe 158
6.1.7 Pufferüberläufe in iOS verhindern 162
6.1.8 Pufferüberläufe finden 167
6.2 Des Pufferüberlaufs kleiner Bruder: Der Pufferunterlauf 168
6.2.1 „Short Write" und „Short Read" 169
6.2.2 Pufferunterläufe verhindern 170
6.3 Formatstring-Schwachstellen 172
6.3.1 Angriff über eine Formatstring-Schwachstelle 172
6.3.2 Objective-C und die Formatstrings 173
6.3.3 Formatstring-Schwachstellen verhindern 173
6.4 Das Standardbeispiel im Licht von Kapitel 6 176

7 Eingaben überprüfen 179

7.1 Eingabefelder für Texte 180
7.2 Dateien aller Art 181
7.3 URLs 183
7.4 Das Standardbeispiel im Licht von Kapitel 7 187
7.4.1 Eingabefelder für Texte 188
7.4.2 Dateien 189
7.4.3 URL 189

8 Rund um die Kommunikation 191

8.1 Interprozess- und Netzwerkkommunikation 191
8.1.1 RPC (Remote Procedure Calls) 191
8.1.2 Signale 192

8.2 Netzwerkverbindungen 193
8.2.1 Authentifizierung des Benutzers 193
8.2.2 AirDrop 199
8.2.3 Gefährliche Umleitungen in Web 200
8.3 Das Standardbeispiel im Licht von Kapitel 8 204

9 Race Conditions und sichere Dateioperationen 205

9.1 Race Conditions 205
9.1.1 Das böse Multitasking 205
9.1.2 „Time of Check/Time of Use"-Schwachstellen 207
9.1.3 Race Conditions beim Signal-Handling 211
9.2 Sichere Dateioperationen 211
9.2.1 Result Codes sind zum Prüfen da! 212
9.2.2 Links können problematisch sein 212
9.2.3 Gefahren durch Case-insensitive Dateisysteme 214
9.2.4 Temporäre Dateien 216
9.2.5 Gefährlich: Dateien in öffentlich beschreibbaren Verzeichnissen 217
9.3 Das Standardbeispiel im Licht von Kapitel 9 218
9.3.1 Race Conditions 218
9.3.2 Dateioperationen 219

10 Kryptografie 221

11 Sicherheit der Benutzeroberfläche 225

11.1 Das A und O: Sichere Default-Einstellungen 225
11.2 Keine gefährlichen Aktionen ohne explizite Zustimmung 226
11.3 Keine Übertragung sensitiver Daten ohne Zustimmung 227
11.4 Vor unwiderruflichen Aktionen wird gewarnt! 227

11.5 Vor Gefahren wird gewarnt! 227
11.6 Sicherheit hat Priorität 228
11.7 Entsprechen Sie den Erwartungen des Benutzers 229

Anhang: Einführung in die Kryptografie 231

A.1 Symmetrische Systeme 232
A.2 Asymmetrische Systeme 234
A.3 Symmetrisch + asymmetrisch = hybride Systeme 235
A.4 Authentikationssysteme 236
A.5 Ein Beispiel für ein hybrides Verfahren 237
A.6 Hash-Funktionen 241
A.7 Digitale Zertifikate 242
A.8 SSL/TLS 243
A.9 Kryptografie unter iOS 245

Link- und Literaturverzeichnis 247

Stichwortverzeichnis 269