

Mobile Application Security

UNIVERSITÄT
LIECHTENSTEIN
Bibliothek

Himanshu Dwivedi
Chris Clark
David Thiel



New York Chicago San Francisco
Lisbon London Madrid Mexico City Milan
New Delhi Sari Juan, Seoul Singapore Sydney Toronto

Contents

Acknowledgments.xix
Introduction.xxi

Part I Mobile Platforms

Chapter 1	Top Mobile Issues and Development Strategies.1
	Top Issues Facing Mobile Devices.	2
	Physical Security.	2
	Secure Data Storage (on Disk).	3
	Strong Authentication with Poor Keyboards.	3
	Multiple-User Support with Security.	4
	Safe Browsing Environment.	4
	Secure Operating Systems.	4
	Application Isolation.	5
	Information Disclosure.	5
	Virus, Worms, Trojans, Spyware, and Malware.	6
	Difficult Patching/Update Process.	6
	Strict Use and Enforcement of SSL.	6
	Phishing.	7
	Cross-Site Request Forgery (CSRF).	7
	Location Privacy/Security.	8
	Insecure Device Drivers.	8
	Multifactor Authentication.	8
	Tips for Secure Mobile Application Development.	9
	Leverage TLS/SSL.	10
	Follow Secure Programming Practices.	10
	Validate Input.	10
	Leverage the Permissions Model Used by the OS.	11
	Use the Least Privilege Model for System Access.	11

	Store Sensitive Information Properly.	11
	Sign the Application's Code.	12
	Figure Out a Secure and Strong Update Process.	12
	Understand the Mobile Browser's Security Strengths and Limitations.	12
	Zero Out the Nonthreats.	13
	Use Secure/Intuitive Mobile URLs.	13
	Conclusion.	14
Chapter 2	Android Security.	15
	Development and Debugging on Android.	17
	Android's Securable IPC Mechanisms.	20
	Activities.	20
	Broadcasts.	20
	Services.	21
	ContentProviders.	21
	Binder.	21
	Android's Security Model.	21
	Android Permissions Review.	22
	Creating New Manifest Permissions.	26
	Intents.	27
	Intent Review.	27
	IntentFilters.	28
	Activities.	29
	Broadcasts.	32
	Receiving Broadcast Intents.	32
	Safely Sending Broadcast Intents.	33
	Sticky Broadcasts.	33
	Services.	34
	ContentProviders.	35
	Avoiding SQL Injection.	37
	Intent Reflection.	37
	Files and Preferences.	38
	Mass Storage.	40
	Binder Interfaces.	40
	Security by Caller Permission or Identity Checking.	41
	Binder Reference Security.	42

Android Security Tools	42
Manifest Explorer	43
Package Play	44
Intent Sniffer	45
Intent Fuzzer	45
Conclusion	46
Chapter 3 The Apple iPhone	49
History	50
The iPhone and OS X	51
Breaking Out, Breaking In	51
iPhone SDK	52
Future	52
Development	52
Decompilation and Disassembly	52
Preventing Reverse-Engineering	56
Security Testing	56
Buffer Overflows	57
* Integer Overflows	57
Format String Attacks	58
Double-Frees	60
Static Analysis	61
Application Format	62
Build and Packaging	62
Distribution: The Apple Store	62
Code Signing	63
Executing Unsigned Code	64
Permissions and User Controls	64
Sandboxing	65
Exploit Mitigation	65
Permissions	66
Local Data Storage: Files, Permissions, and Encryption	66
SQLite Storage	67
iPhone Keychain Storage	68
Shared Keychain Storage	69
Adding Certificates to the Certificate Store	70
Acquiring Entropy	70

Networking71
The URL Loading API.72
NSStreams.73
Peer to Peer (P2P).74
Push Notifications, Copy/Paste, and Other IPC.75
Push Notifications.75
UIPasteboard.76
Conclusion.77
Chapter 4 Windows Mobile Security.79
Introduction to the Platform.80
Relation to Windows CE.80
Device Architecture.81
Device Storage.83
Kernel Architecture.83
Memory Layout84
Windows CE Processes.85
Services.86
Objects.86
Kernel Mode and User Mode.88
Development and Security Testing.90
Coding Environments and SDKs.90
Emulator.91
Debugging.94
Disassembly.97
Code Security.100
Application Packaging and Distribution104
Permissions and User Controls.106
Privileged and Normal Mode.107
Authenticode, Signatures, and Certificates.107
Public Key Cryptography.108
Running Applications.110
Locking Devices.111
Managing Device Security Policy.113
Local Data Storage.114
Files and Permissions.114
Stolen Device Protections.116

|) j

	Structured Storage.116
	Encrypted and Device Secured Storage.116
	Networking.117
	Connection Manager.118
	WinSock118
	IrDA118
	Bluetooth.119
	HTTP and SSL119
	Conclusion.119
Chapter 5	BlackBerry Security.121
	Introduction to Platform.122
	BlackBerry Enterprise Server (BES)123
	BlackBerry Internet Service (BIS).123
	Device and OS Architecture.124
	Development and Security Testing.125
	Coding Environment.125
	Simulator.126
	"Debugging.127
	Disassembly.129
	Code Security.131
	Application Packaging and Distribution.132
	Permissions and User Controls.134
	RIM Controlled APIs.135
	Carrier and MIDLet Signatures.140
	Handling Permission Errors in MI DP Applications.....	.141
	Locking Devices.142
	Managing Application Permissions.143
	Local Data Storage.143
	Files and Permissions.144
	Programmatic File System Access.144
	Structured Storage.145
	Encrypted and Device Secured Storage.146
	Networking.148
	Device Firewall.148
	SSL and WTLS148
	Conclusion.149

Chapter 6	Java Mobile Edition Security151
	Standards Development152
	Configurations, Profiles, and JSRs153
	Configurations154
	Profiles155
	Optional Packages156
	Development and Security Testing157
	Configuring a Development Environment and Installing New Platforms158
	Emulator160
	Emulator and Data Execution Protection160
	Reverse Engineering and Debugging162
	Hiding Cryptographic Secrets165
	Code Security168
	Application Packaging and Distribution170
	Permissions and User Controls175
	Data Access178
	Conclusion179
Chapter 7	SymbianOS Security181
	Introduction to the Platform182
	Device Architecture183
	Device Storage185
	Development and Security Testing186
	Development Environment186
	Software Development Kits187
	Emulator188
	Debugging190
	IDA Pro190
	Code Security191
	Symbian C++192
	PIPS and OpenC199
	Application Packaging200
	Executable Image Format200
	Installation Packages202
	Signatures203
	Symbian Signed204
	Installation206

Permissions and User Controls.	207
Capabilities Overview.	207
Executable Image Capabilities.	209
Process Capabilities.	209
Capabilities Between Processes.	210
Interprocess Communication.	211
Client/Server Sessions.	211
Shared Sessions.	216
Shared Handles.	217
Persistent Data Storage.	217
File Storage.	218
Structured Storage.	219
Encrypted Storage.	220
Conclusion.	223
Chapter 8 WebOS Security.	225
Introduction to the Platform.	226
WebOS System Architecture.	227
'Model-View-Controller.	230
Stages and Scenes, Assistants and Views.	230
Development and Security Testing.	231
Developer Mode.	232
Accessing Linux.	232
Emulator.	233
Debugging and Disassembly.	234
Code Security.	237
Script Injection.	237
Direct Evaluation.	238
Programmatic Data Injection.	240
Avoiding innerHTML and updated Injections.	241
Template Injection.	242
Local Data Injection.	243
Application Packaging.	246
Permissions and User Controls.	247
Storage.	247
Networking.	250
Conclusion.	250

Part II Mobile Services

Chapter 9	WAP and Mobile HTML Security.	251
	WAP and Mobile HTML Basics.	253
	Authentication on WAP/Mobile HTML Sites.	254
	Encryption.	257
	WAP 1.0.	258
	SSL and WAP 2.0.	259
	Application Attacks on Mobile HTML Sites.	260
	Cross-Site Scripting.	260
	SQL Injection.	264
	Cross-Site Request Forgery.	266
	HnP Redirects.	270
	Phishing.	272
	Session Fixation.	272
	Non-SSL Login.	273
	WAP and Mobile Browser Weaknesses.	273
	Lack of HTTPOnly Flag Support	274
	Lack of SECURE Flag Support	274
	Handling Browser Cache	274
	WAP Limitations.	275
	Conclusion.	275
Chapter 10	Bluetooth Security.	277
	Overview of the Technology.	278
	History and Standards.	278
	Common Uses.	279
	Alternatives.	279
	Future.	281
	Bluetooth Technical Architecture.	281
	Radio Operation and Frequency.	281
	Bluetooth Network Topology.	282
	Device Identification.	283
	Modes of Operation.	283
	Bluetooth Stack.	285
	Bluetooth Profiles.	286

	Bluetooth Security Features.	287
	Pairing.	288
	Traditional Security Services in Bluetooth.	290
	Security "Non-Features".	294
	Threats to Bluetooth Devices and Networks.	294
	Bluetooth Vulnerabilities.	295
	Bluetooth Versions Prior to v1.2.	296
	Bluetooth Versions Prior to v2.1.	296
	All Versions.	296
	Recommendations.	297
Chapter 11	SMS Security.	299
	Overview of Short Message Service.	301
	Overview of Multimedia Messaging Service.	304
	Wireless Application Protocol (WAP).	306
	Protocol Attacks.	308
	Abusing Legitimate Functionality.	310
	Attacking Protocol Implementations.	321
	Application Attacks.	324
	iPhone Safari.	325
	Windows Mobile MMS.	325
	Motorola RAZR JPG Overflow.	326
	Walkthroughs.	326
	Sending PDUs.	327
	ConvertingXMLtoWBXML.	329
	Conclusion.	329
Chapter 12	Mobile Geolocation.	331
	Geolocation Methods.	332
	Tower Triangulation.	332
	GPS.	333
	802.11.	333
	Geolocation Implementation.	334
	Android.	334
	iPhone.	336
	WindowsMobile.	337
	Geolocation Implementation.	337
	Symbian.	337
	BlackBerry.	338

	Risks of Geolocation Services.	339
	Risks to the End User.	340
	Risks to Service Providers.	341
	Geolocation Best Practices.	341
Chapter 13	Enterprise Security on the Mobile OS.	343
	Device Security Options.	344
	PIN.	345
	Remote Wipe.	346
	Secure Local Storage.	347
	Apple iPhone and Keychain.	347
	Security Policy Enforcement.	348
	Encryption.	350
	Full Disk Encryption.	350
	E-mail Encryption.	350
	File Encryption.	351
	Application Sandboxing, Signing, and Permissions.	352
	Application Sandboxing.	352
	Application Signing.	354
	Permissions.	356
	Buffer Overflow Protection.	357
	Windows Mobile.	358
	iPhone.	359
	Android.	359
	BlackBerry.	359
	Security Feature Summary.	360
	Conclusion.	360
Part III	Appendixes	
Appendix A	Mobile Malware.	363
	A Tour of Important Past Malware.	364
	Cabir.	365
	Commwarrior.	365
	Beselo.B.	365
	Trojan.Redbrowser.A.	365
	WinCE/Brador.a.	366

	WinCE/Infojack	366
	SMS.Python.Flotker	366
	Yxes.A	366
	Others	367
	Threat Scenarios	367
	Fake Firmware	367
	Classic Trojans	367
	Worms	368
	Ransomware	368
	Mitigating Mobile Malware Mayhem	369
	For End Users	369
	For Developers and Platform Vendors	369
Appendix B	Mobile Security Penetration Testing Tools	371
	Mobile Platform Attack Tools and Utilities	372
	Manifest Explorer	372
	Package Play	373
	Intent Sniffer	374
	- Intent Fuzzer	375
	pySimReader	376
	Browser Extensions	377
	WMLBrowser	377
	User Agent Switcher	377
	FoxyProxy	377
	TamperData	379
	Live HTTP Headers	379
	Web Developer	380
	Firebug	381
	Networking Tools	381
	Wireshark	381
	Tcpdump	382
	Scapy	384
	Web Application Tools	384
	WebScarab	384
	Gizmo	386

Fuzzing Frameworks.	387
Peach.	387
Sulley.	387
General Utilities.	388
Hachoir.	388
VBinDiff.	388
Index.	391