



Contents

About the Author	vii
Acknowledgments	ix
Introduction	xvii
Chapter 1 Understanding the Threats	3
Quantifying the Threat	4
The Malware Threat	4
Direct Attack	6
Data-Communication Interception	9
Authentication Spoofing and Sniffing	11
Physical Compromise	12
Mobile Device Enterprise Infrastructure	14
PC and LAN Connectivity	17
Fundamental Changes in Security Strategy	20
Protecting the Mobile Device Itself	21
Enforcing Compliance on the Mobile Device	22
Addressing Security Deficiencies Automatically	22
Implementing Layered Security	22
Controlling and Protecting Data	22
Things to Remember	22
Chapter 2 Understanding the Devices	25
BlackBerrys	26
BlackBerry Business Phones	26
BlackBerry Handheld Devices	30
BlackBerry-Enabled Devices	34
Pocket PCs	35
Dell Axim Pocket PCs	36
HP Pocket PCs	37



xii Contents

	Palm Pocket PCs	38
	Motorola Pocket PC	39
	Palm Handhelds	40
	Palm Smartphones	41
	Cell Phones	42
	Symbian OS Cell Phones	42
	Non-Symbian OS Cell Phones	43
	Things to Remember	43
Chapter 3	Exploiting BlackBerry Devices	47
	Malware Is Threatening Your BlackBerry	48
	Analyzing a Malware Attack	49
	Gathering Information	50
	Setting Up for the Attack and Covering His Tracks	50
	Launching the Attack	54
	Protecting Against This Attack	57
	Learning about New Vulnerabilities	60
	BlackBerry Antivirus Software	62
	Attacking a BlackBerry Directly	64
	Attacking via IP Address	64
	Attacking via Malware	70
	Antimalware Applications	70
	Enterprise-Grade Firewall with IDS/IPS	71
	The BlackBerry Firewall	72
	Ensuring the Device Has the Latest Updates	78
	Educating Users about Risks	79
	Intercepting BlackBerry Communication	80
	What Data Is Being Transmitted?	82
	How Is Data Being Transmitted?	82
	Carrier Internet Access	83
	Bluetooth	85
	The BlackBerry Wi-Fi Interface	87
	Physically Compromising a BlackBerry by	
	Spoofing and Intercepting Authentication	87
	How Physical Compromise Happens	88
	Preventing Physical Compromise	89
	Protecting a Stand-Alone BlackBerry	90
	Preventing Unauthorized Access	90
	The Truth About Wiping A Lost or Stolen BlackBerry	91
	Implementing Content Protection	91
	Spoofing and Intercepting Authentication	92
	BlackBerry Security Checklist	93
	Things to Remember	94
Chapter 4	Hacking the Supporting BlackBerry Infrastructure	95
	Good and Bad: A Conduit to Your LAN	95
	Understanding the BlackBerry Infrastructure	96
	BlackBerry Infrastructure Components	96
	Infrastructure Design Considerations	97

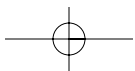


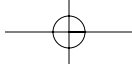
Attacking the BlackBerry Infrastructure	99
The Attacker's Side of the Story	101
Insecure Server Configuration	101
Insecure Topology	103
BBProxy	104
Things to Remember	109
Chapter 5 Protecting Your PC and LAN from BlackBerrys	111
Controlling Data Is Critical	112
How Companies Lose Control of Data	113
How to Control Data	116
Create and Communicate a Formal Policy	116
Enforce Security Policies with Available Technology	117
Threats from BlackBerry-Provided Internet Access	119
Internet Attack	120
The Attacker's Side of the Story	121
Preventing the Attack	130
Stay Up-to-Date with Patches	131
Use a Personal Firewall	133
Controlling Data Coming from a BlackBerry	134
Analyze the Data Coming from the BlackBerry	134
Analyze the Data as It Resides on the BlackBerry	137
Control Which Devices Can Connect to Your Enterprise PCs	137
Things to Remember	138
Chapter 6 Exploiting PDAs	141
Corrupting Your PDA with Malware	142
Backdoor Malware for the Pocket PC	142
Other PDA Malware	156
PDA Antimalware Programs	157
Kaspersky Security for PDAs	157
JSJ Antivirus	157
Trend Micro Mobile Security	159
Symantec AntiVirus for Handhelds	159
McAfee VirusScan Mobile	160
Targeting a PDA Directly	161
Finding a PDA	161
Making a PDA Stealthy	164
PDA Firewall Applications	165
Trend Micro Mobile Security (for PDA)	165
Aircscanner Mobile Firewall (for Pocket PC)	165
Intercepting PDA Communication	167
Surfing the Internet at Public Wi-Fi Hotspots	167
Using IM and Checking Email at Public Wi-Fi Hotspots	170
Using Virtual Private Networks (VPN) to Secure Data	176
PDA Authentication Spoofing and Interception	177
Sniffing Email Authentication	177
Stealing Credentials with Access Point (AP) Phishing	180
Intercepting Authentication via SSL Man-in-the-Middle	185



xiv Contents

Compromising the PDA Physically	191
Controlling Access to the PDA	192
Palm PDA Security	192
Pocket-PC Security	194
Encrypting Data on the PDA	195
Palm PDA Encryption	196
Pocket-PC Encryption	196
Things to Remember	198
Chapter 7 Hacking the Supporting PDA Infrastructure	201
Connecting a PDA to the LAN Is Good and Bad	201
You Get What You Pay For	202
Strengthen the Wireless Infrastructure	204
Using PDA VPN Clients to Protect the Infrastructure	207
Be Smart about Providing Access	207
Protect Credentials — Protect the Infrastructure	208
Control Access to Email with VPN Clients	208
Things to Remember	209
Chapter 8 Protecting Your PC and LAN from PDAs	211
Connecting PDAs to Enterprise Resources	211
Transferring Data with a Pocket PC	211
Transferring Data with a Palm Device	214
Why Transferring Data Is a Problem	216
PDAs May Be Contagious	220
Good Intentions, Bad Results	220
Anatomy of an Infection	221
Infection by a Pocket PC	222
Infection by a Palm Device	225
Preventing PDAs from Bringing Malware into the Enterprise	228
Ensure PCs Are Using Antivirus Software Properly	228
Ensure All PDAs Contain Antivirus Software	230
Control Whether PDAs Can Connect to PCs	231
Centralized Management Tools for the PDA	237
Things to Remember	238
Chapter 9 Exploiting Cell Phones	241
Cell-Phone Malware	242
The King of All Cell-Phone Malware?	243
FlexiSpy: Trojan or Valid Software?	243
Other Cell-Phone Malware	245
Stopping Cell-Phone Malware	245
Trend Micro Mobile Security for Symbian	246
Symantec Mobile Security for Symbian	247
F-Secure Mobile Security	247
Stealing Data via Bluetooth	248
Discovering a Cell Phone via Bluetooth	249
Attacking a Cell Phone via Bluetooth	253
Preventing Bluetooth Attacks	258





Contents xv

Intercepting Cell-Phone Communication	258
Physical Compromise and Cell-Phone Authentication Spoofing	260
A Real-World Example	261
Analyzing Physical Tampering	261
Preventing Physical Tampering	264
Spoofing Authentication with a Cell Phone	265
Things to Remember	268
Chapter 10 Protecting the Enterprise PC and LAN from Cell Phones	269
Cell Phones May Bring in Malware	269
How It Happens	270
How to Stop the Attack	271
Exposing Enterprise Email	272
A Creative Way to Access Enterprise Email	272
Prevent Email Forwarding	275
Exporting Enterprise Data and Clandestine Data Gathering	275
Mobile Phone Tools	275
Clandestine Information Gathering	276
Things to Remember	276
Index	277

