Contents

About This Book xi
Foreword xiii
About the Authors xv
Author’s Acknowledgements xxi
Symbian Press Acknowledgements xxiii

Part 1 Introduction to Symbian OS Platform Security 1

1 Why a Secure Platform? 3
  1.1 User Expectations of Mobile Phone Security 3
  1.2 What the Security Architecture Should Provide 4
  1.3 Challenges and Threats to Mobile Phone Security 6
  1.4 How Symbian OS Platform Security Fits into the Value Chain 12
  1.5 How Application Developers Benefit from the Security Architecture 16

2 Platform Security Concepts 17
  2.1 Background Security Principles 17
  2.2 Architectural Goals 20
  2.3 Concept 1: The Process is the Unit of Trust 22
  2.4 Concept 2: Capabilities Determine Privilege 27
  2.5 Concept 3: Data Caging for File Access 37
  2.6 Summary 40
# CONTENTS

## Part 2  Application Development for Platform Security  

43

### 3 The Platform Security Environment  

45

- Building Your Application  
- Developing on the Emulator  
- Packaging Your Application  
- Testing on Mobile Phone Hardware  
- Summary  

### 4 How to Write Secure Applications  

61

- What Is a Secure Application?  
- Analyzing the Threats  
- What Countermeasures Can Be Taken?  
- Implementation Considerations  
- Summary  

### 5 How to Write Secure Servers  

83

- What Is a Secure Server?  
- Server Threat Modeling  
- Designing Server Security Measures  
- Server Implementation Security Considerations  
- Summary  

### 6 How to Write Secure Plug-ins  

111

- What Is a Secure Plug-In?  
- Writing Secure Plug-ins  
- Plug-in Implementation Considerations  
- Summary  

### 7 Sharing Data Safely  

129

- Introduction to Sharing Data  
- Categories of Data  
- Deciding the Level of Trust  
- Attacks on Data and Countermeasures  
- Using System Services  
- Summary  

## Part 3  Managing Platform Security Attributes  

155

### 8 Native Software Installer  

157

- Introduction to the Native Software Installer  
- Validating Capabilities  
- Identifiers, Upgrades, Removals and Special Files  
<table>
<thead>
<tr>
<th>Contents</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>8.4 SIS File Changes for Platform Security</td>
<td>177</td>
</tr>
<tr>
<td>8.5 Installing to and from Removable Media</td>
<td>181</td>
</tr>
<tr>
<td>8.6 Summary</td>
<td>184</td>
</tr>
<tr>
<td>9 Enabling Platform Security</td>
<td>187</td>
</tr>
<tr>
<td>9.1 Responsibilities in Granting Capabilities</td>
<td>187</td>
</tr>
<tr>
<td>9.2 Overview of the Signing Process</td>
<td>189</td>
</tr>
<tr>
<td>9.3 Step-by-step Guide to Signing</td>
<td>192</td>
</tr>
<tr>
<td>9.4 Revocation</td>
<td>202</td>
</tr>
<tr>
<td>9.5 Summary</td>
<td>204</td>
</tr>
<tr>
<td>Part 4 The Future of Mobile Device Security</td>
<td>205</td>
</tr>
<tr>
<td>10 The Servant in Your Pocket</td>
<td>207</td>
</tr>
<tr>
<td>10.1 Crystal-Ball Gazing</td>
<td>207</td>
</tr>
<tr>
<td>10.2 Convergence, Content and Connectivity</td>
<td>207</td>
</tr>
<tr>
<td>10.3 Enabling New Services</td>
<td>209</td>
</tr>
<tr>
<td>10.4 New Security Technologies</td>
<td>211</td>
</tr>
<tr>
<td>10.5 Summary</td>
<td>217</td>
</tr>
<tr>
<td>Appendix A Capability Descriptions</td>
<td>219</td>
</tr>
<tr>
<td>Appendix B Some Cryptography Basics</td>
<td>225</td>
</tr>
<tr>
<td>Appendix C The Software Install API</td>
<td>229</td>
</tr>
<tr>
<td>Glossary</td>
<td>233</td>
</tr>
<tr>
<td>References</td>
<td>237</td>
</tr>
<tr>
<td>Index</td>
<td>239</td>
</tr>
</tbody>
</table>