BLACKJACKING: SECURITY THREATS TO BLACKBERRY DEVICES, PDAS, AND CELL PHONES IN THE ENTERPRISE

About the Author.
Acknowledgments.
Introduction.

Chapter 1 Understanding the Threats.
Quantifying the Threat.
The Malware Threat.
Direct Attack.
Data-Communication Interception.
Authentication Spoofing and Sniffing.
Physical Compromise.
Mobile Device Enterprise Infrastructure.
PC and LAN Connectivity.
Protecting the Mobile Device Itself.
Enforcing Compliance on the Mobile Device.
Addressing Security Deficiencies Automatically.
Implementing Layered Security.
Controlling and Protecting Data.
Things to Remember.

Chapter 2 Understanding the Devices.
BlackBerrys.
BlackBerry Business Phones.
BlackBerry Handheld Devices.
BlackBerry-Enabled Devices.
Pocket PCs.

BUY ONLINE AT: http://www.itgovernance.co.uk/products/1255
Dell Axim Pocket PCs.
HP Pocket PCs.
Palm Pocket PCs.
Motorola Pocket PC.
Palm Handhelds.
Palm Smartphones.
Cell Phones.
Symbian OS Cell Phones.
NonSymbian OS Cell Phones.

Things to Remember.

**Chapter 3 Exploiting BlackBerry Devices.**

Malware Is Threatening Your BlackBerry.

Analyzing a Malware Attack.

Gathering Information.

Setting Up for the Attack and Covering His Tracks.

Launching the Attack.

Protecting Against This Attack.

Learning about New Vulnerabilities.

**BlackBerry Antivirus Software.**

Attacking a BlackBerry Directly.

Attacking via IP Address.

Attacking via Malware.

Antimalware Applications.

Enterprise-Grade Firewall with IDS/IPS.

The BlackBerry Firewall.

Ensuring the Device Has the Latest Updates.

Educating Users about Risks.

Intercepting BlackBerry Communication.
What Data Is Being Transmitted?
How Is Data Being Transmitted?
Carrier Internet Access.
Bluetooth.
The BlackBerry Wi-Fi Interface.
Physically Compromising a BlackBerry by Spoofing and Intercepting Authentication.
How Physical Compromise Happens.
Preventing Physical Compromise.
Protecting a Stand-Alone BlackBerry.
Preventing Unauthorized Access.
The Truth About Wiping A Lost or Stolen BlackBerry.
Implementing Content Protection.
Spoofing and Intercepting Authentication.
BlackBerry Security Checklist.
Things to Remember.

Chapter 4 Hacking the Supporting BlackBerry Infrastructure.
Good and Bad: A Conduit to Your LAN.
Understanding the BlackBerry Infrastructure.
BlackBerry Infrastructure Components.
Infrastructure Design Considerations.
Attacking the BlackBerry Infrastructure.
The Attackers Side of the Story.
Insecure Server Configuration.
Insecure Topology.
BBProxy.
Things to Remember.

Chapter 5 Protecting Your PC and LAN from BlackBerrys.
Controlling Data Is Critical.

BUY ONLINE AT: http://www.itgovernance.co.uk/products/1255
How Companies Lose Control of Data.

How to Control Data.

Create and Communicate a Formal Policy.

Enforce Security Policies with Available Technology.

Threats from BlackBerry-Provided Internet Access.

Internet Attack.

The Attackers Side of the Story.

Preventing the Attack.

Stay Up-to-Date with Patches.

Use a Personal Firewall.

Controlling Data Coming from a BlackBerry.

Analyze the Data Coming from the BlackBerry.

Analyze the Data as It Resides on the BlackBerry.

Control Which Devices Can Connect to Your Enterprise PCs.

Things to Remember.

**Chapter 6 Exploiting PDAs.**

Corrupting Your PDA with Malware.

Backdoor Malware for the Pocket PC.

Other PDA Malware.

PDA Antimalware Programs.

Kaspersky Security for PDAs.

JSJ Antivirus.


Symantec AntiVirus for Handhelds.

McAfee VirusScan Mobile.

Targeting a PDA Directly.

Finding a PDA.

Making a PDA Stealthy.
PDA Firewall Applications.
Trend Micro Mobile Security (for PDA).
Airscanner Mobile Firewall (for Pocket PC).
Intercepting PDA Communication.
Surfing the Internet at Public Wi-Fi Hotspots.
Using IM and Checking Email at Public Wi-Fi Hotspots.
Using Virtual Private Networks (VPN) to Secure Data.
PDA Authentication Spoofing and Interception.
Sniffing Email Authentication.
Stealing Credentials with Access Point (AP) Phishing.
Intercepting Authentication via SSL Man-in-the-Middle.
Compromising the PDA Physically.
Controlling Access to the PDA.
Palm PDA Security.
Pocket-PC Security.
Encrypting Data on the PDA.
Palm PDA Encryption.
Pocket-PC Encryption.
Things to Remember.

**Chapter 7 Hacking the Supporting PDA Infrastructure.**

Connecting a PDA to the LAN Is Good and Bad.
You Get What You Pay For.
Strengthen the Wireless Infrastructure.
Using PDA VPN Clients to Protect the Infrastructure.
Be Smart about Providing Access.
Protect Credentials  Protect the Infrastructure.
Control Access to Email with VPN Clients.
Things to Remember.
Chapter 8 Protecting Your PC and LAN from PDAs.

Connecting PDAs to Enterprise Resources.

Transferring Data with a Pocket PC.

Transferring Data with a Palm Device.

Why Transferring Data Is a Problem.

PDAs May Be Contagious.

Good Intentions, Bad Results.

Anatomy of an Infection.

Infection by a Pocket PC.

Infection by a Palm Device.

Preventing PDAs from Bringing Malware into the Enterprise.

Ensure PCs Are Using Antivirus Software Properly.

Ensure All PDAs Contain Antivirus Software.

Control Whether PDAs Can Connect to PCs.

Centralized Management Tools for the PDA.

Things to Remember.

Chapter 9 Exploiting Cell Phones.

Cell-Phone Malware.

The King of All Cell-Phone Malware?

FlexiSpy: Trojan or Valid Software?

Other Cell-Phone Malware.

Stopping Cell-Phone Malware.


Symantec Mobile Security for Symbian.

F-Secure Mobile Security.

Stealing Data via Bluetooth.

Discovering a Cell Phone via Bluetooth.

Attacking a Cell Phone via Bluetooth.

BUY ONLINE AT: http://www.itgovernance.co.uk/products/1255
Preventing Bluetooth Attacks.

Intercepting Cell-Phone Communication.

Physical Compromise and Cell-Phone Authentication Spoofing.

A Real-World Example.

Analyzing Physical Tampering.

Preventing Physical Tampering.

Spoofing Authentication with a Cell Phone.

Things to Remember.

Chapter 10 Protecting the Enterprise PC and LAN from Cell Phones.

Cell Phones May Bring in Malware.

How It Happens.

How to Stop the Attack.

Exposing Enterprise Email.

A Creative Way to Access Enterprise Email.

Prevent Email Forwarding.

Exporting Enterprise Data and Clandestine Data Gathering.

Mobile Phone Tools.

Clandestine Information Gathering.

Things to Remember.

Index.