

PDA insecurity

Insecurity in a mobile world

Bryan Glancey



Black Hat Briefings

Agenda

- PocketPC Overview
 - Registry
 - Synchronization
 - Autorun
 - HP 5455 Biometric issue
- Palm Overview
- General Issues
- Conclusion



PocketPC

- ActiveSync
 - USB/Serial
 - BlueTooth
 - TCP/IP



PocketPC Toolkit

- Registry Editors
 - www.pocketpcdn.com/articles/registry.html
- RedBack
 - www.atstake.com/research/tools/forensic/
- Snort – Airsnort
 - Airsnort.shmoo.com
 - www.snort.org



PocketPC Registry

- Windows Like Registry Settings
 - Edit the registry remotely
 - Edit it on the device
 - Password Screen Control
 - <http://support.microsoft.com/default.aspx?scid=kb;en-us;314989>
 - Interesting Values



File Zoom Tools Help

Start 2h 3:27 ok

.. Back/Up

0) TimeOut
1) Redirect
2) NSSavedRedirect
3) Group

Count: 4

Path HKEY_CLASSES_ROOT\ControlPanel\Pas

Key Password

Class

Type REG_SZ: A null-terminated Unicode strin

Entry \"Windows\BioSwipe.cpl\"

Edit Open

earch Results - Mi... DEF CON 11 Sched... 314989 - Let Me In... PocketGear.com - P... kilmist - Microsoft In...



Security Related Values

- HKEY_LOCAL_MACHINE\Comm
- HKEY_LOCAL_MACHINE\Drivers
- HKEY_LOCAL_MACHINE\HARDWARE
- HKEY_LOCAL_MACHINE\SYSTEM
- HKEY_LOCAL_MACHINE\Init
- HKEY_LOCAL_MACHINE\WDMDrivers
- [HKEY_CLASSES_ROOT\.cpl]
(default) = "cplfile"

[HKCR\cplfile\Shell\Open\Command]
(default) = "\Windows\ctlpnl.exe %1"



Where to get more information?

- Microsoft
 - How to switch the password screen
 - Q314989 - Let Me In: Pocket PC Password User Interface Redirect Sample
 - <http://support.microsoft.com/default.aspx?scid=kb;en-us;314989>



PocketPC attacks

- AutoRUN
- Activesync cradle
 - Data security is unidirectional – you can put a system password on PocketPC but not on Laptop
- ActiveSync DOS
 - <http://www.irmpic.com/advisories> The (**ActiveSync**) service runs on TCP port 5679 and by connecting to this port and sending...
- Removable media



Example: HP Ipaq 5455

hp iPAQ h5400



**mouse
commands**

Ideal for the mobile professional: Security features with the Biometric Fingerprint Reader as well as compatibility with familiar Microsoft Pocket PC 2002 applications such as Outlook, Word, and Excel. IPAQ Task Manager, File Store and Backup add functionality and user control.



Black Hat Briefings

5455 Weaknesses

- Synchronization Security
 - Spontaneous Password Lapses
 - <http://forums.itrc.hp.com/cm/QuestionAnswer/1,,0x504cb82b2d63d71190080090279cd0f9,00.html>
- Removable Media Security
 - New definition of 'Plug & Play'



AUTORUN Killer

- Autorun on Memory card insertion
 - http://msdn.microsoft.com/library/default.asp?url=/library/en-us/apcguide/htm/distrib_6.asp



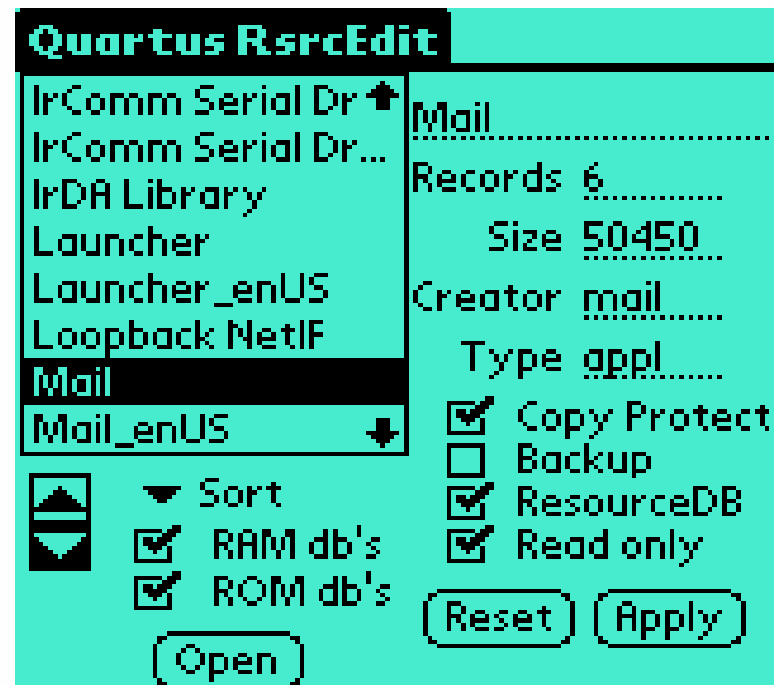
Palm

- HotSync Vulnerabilities
 - NotSync
 - <http://www.atstake.com/research/advisories/2000/a092600-1.txt>
- PDD



Palm Toolkit

- PDD
- NotSync
- PDA Seizure
 - <http://www.paraben-forensics.com/index.html>
- RsrcEdit
 - <http://www.quartus.net/products/rsrcredit/>
 - File Manager/editor for PalmOS



Palm

- Palm Memo hiding Vulnerability
 - www.securityfocus.com/archive/1/328549
 - Any File Manager/Editor can view/edit hidden memos



PDA Holes - Overview

- Removable Media
- Reset programs
- Synchronization Programs
- No Security Standards
 - User picks password
 - Dictionary Attacks
 - Locking optional
 - No Encryption
- Security Varies from manufacturer to manufacturer – Even within same operating system



PDA Connection Points

- USB/Serial (TCP/IP)
- 802.11
- Bluetooth



General Synch Vulnerabilities

- TCP/IP (Wireless)
 - All synchronization traffic is unencrypted
 - Easy to sniff the data
- Bluetooth
 - Incomplete security
 - Redback Software allows you to discover “undiscoverable” Bluetooth devices



Questions

- Thanks

