PDA insecurity

Insecurity in a mobile world

Bryan Glancey
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](http://support.microsoft.com/default.aspx?scid=kb;en-us;314989)
    - Interesting Values
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.irmplc.com/advisories The (ActiveSync) service runs on TCP port 5679 and by connecting to this port and sending…
- Removable media
Example: HP iPaq 5455

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.
5455 Weaknesses

- Synchronization Security
  - Spontaneous Password Lapses
    - [http://forums.itrc.hp.com/cm/QuestionAnswer/1,,0x504cb82b2d63d71190080090279cd0f9,00.html](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
Palm

- HotSync Vulnerabilities
  - NotSync

- PDD
Palm Toolkit

- PDD
- NotSync
- PDA Seizure
- RssrcEdit
  - File Manager/editor for PalmOS
Palm

- Palm Memo hiding Vulnerability
  - [www.securityfocus.com/archive/1/328549](http://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 “undiscourable” Bluetooth devices
Questions

• Thanks