# Introduction to Mobile Device Insecurity

Black Hat Europe 2004 Briefings Thursday, May 20, 11:30am - 12:45pm

Joe Grand Grand Idea Studio, Inc. joe@grandideastudio.com

#### Goals

- Understand <u>classes</u> of problems
- Learn security risks and protection methods
- Education by demonstration



### By The Numbers...

- Palm OS: 41.8% of handheld market, 30 million units sold to date
- IDC: 533.4 million mobile phones worldwide in 2003
- IDC: 30 million smartphones (cell + PDA) to ship in 2004
- VDC: 75 million Java-enabled devices to ship in 2004



### The Major Players: Palm OS

 Ex.: Palm, Handspring, Sony, IBM, Kyocera, Samsung, Qualcomm, Franklin Covey, TRG, Symbol, HandEra









## The Major Players: Windows CE / Pocket PC

 Ex.: Microsoft, HP, Compaq, Sony, Cingular, Gateway, JVC, Dell, Fujitsu, Toshiba, Panasonic, Symbol











## The Major Players: Symbian OS

 Ex.: Nokia, Psion, Sony Ericsson, Motorola, Siemens, FOMA, Panasonic









#### **Common Uses**

- Personal
  - Phone numbers, memos, to do lists, diaries
- Security/Network Admin
  - IP addresses, network maps, usernames & passwords, authentication tokens, one-time-password generation
- Medical
  - Patient information, medications, treatments
- Government/Military
  - Schedules, sensitive/secret information



#### **Common Uses 2**

- Wireless
  - WWW, E-mail, Instant Messaging, e-commerce



#### **Current Risks**

- Mixing business with pleasure
- Admin, users not aware of the existing security problems
- Most devices have no security framework
  - No access control or data/memory protection
  - Hardware can be directly accessed by the user through software
  - No physical secure hardware design methods



#### **Current Risks 2**

- Data is stored as plaintext in accessible memory
- Being employed in security-related apps
  - One-time-passwords & authentication tokens
  - Storage of private/confidential information
  - E-commerce, wireless payment
- Cannot have secure apps on top of an insecure platform
  - Third-party apps are simply a road-block for an attacker, not 100% protection



#### **Current Risks 3**

- "Always on" technologies
  - Ex.: Network, WiFi, Bluetooth, IR
  - Open to the outside world...all the time
- External memory cards
  - Supported on most all new mobile devices
  - Easy to steal
  - Some devices load apps into memory upon insertion
- Existing security mechanisms are weak and/or flawed



#### The Good News

- New devices seem to be taking security more seriously
- Some vendors used to get defensive...now they are actually incorporating changes
- Security features designed into Palm OS 6.0
- Windows Mobile 2003, Linux, Java devices provide abstraction of user v. OS v. hardware
- But...device should still be fully tested and analyzed before deployment



#### **Access to Data**

- Double-edged sword
  - Could be used for good or evil
- System Password Retrieval
- Debug Modes and Sync Interfaces
- Physical Access



## System Password Retrieval

- Power-on and data protection using a password
- Often weak obfuscation, not encryption
- Password re-use
  - Human nature easier to remember a single password

Can lead to attacks on other computers, ATM,

voicemail







## System Password Retrieval: Palm OS < 4.0

- Max. 32 characters ASCII
- Reversible obfuscation method (XOR against constant block)
- Can retrieve password/hash [1]:
  - During HotSync operation (IR, Serial, Network)
  - "Unsaved Preferences" database
  - On host PC: \Palm\users.dat
  - On host Mac: Palm: Users: Palm Users
  - On Palm: ppwdump, NotSync



## System Password Retrieval 2: Palm OS < 4.0

- Demo: Retrieve and decode password using ppwdump
- Recommendations:
  - Upgrade to device running newer version of Palm OS





## System Password Retrieval: Palm OS >= 4.0

- Max. 32 characters ASCII
- Encoded block is 128-bit MD5 hash
- One-way hash (not reversible)
- Dictionary attack using common words
  - Take advantage of short passwords

## System Password Retrieval: Windows CE / Pocket PC

- ActiveSync used for all communication between PC and device
  - Available through serial, USB, IR, TCP/IP, Bluetooth
  - No confidentially of transferred data
- Reversible obfuscation method (XOR against constant)
- Can retrieve password/hash [2]:
  - In host PC registry: hkey\_current\_user\software\
    Microsoft\Windows Ce Services\Partners



## System Password Retrieval: Windows CE / Pocket PC 2

- On some devices, 4-digit PIN used for authentication can be brute-forced manually or programmatically [3]
- Pocket PC registry accessible by any user on the device
  - Ex.: PHM Registry Editor, PPTools
  - Ex.: PPP network passwords stored in plaintext



## System Password Retrieval: Windows CE / Pocket PC 3

- Can change Control Panel Applet (cpl) entry in registry to load another app on power-up
  - Microsoft "Let Me In" example, Q314989, demonstrates how to redirect password screen

## System Password Retrieval: Mobile Phones

- Password is usually limited to 4 digits
  - Ex: Last 4 digits of phone number, pattern (0000, 1111, 1234, etc.)
  - Users often use same PIN on phone as they do for voicemail and ATMs
- Most, if not all, have diagnostic/administration menu
  - Some accessible through keypad, others with hardware cable
  - Ex.: Nokia DCT-3 and DCT-4 series phones



### Palm Backdoor Debug Mode

- Exists for debugging during app development
- Can use to bypass "System Lockout" functionality [4]
- Can install/delete/run apps, view raw memory, hard reset, export databases
- Third-party security apps at risk
  - Obtain plaintext components from memory, install "keystroke monitor" to retrieve passwords



### Palm Backdoor Debug Mode 2

- Demo: Display databases and memory
- Demo: pdd to retrieve exact device RAM image
- Recommendations:
  - Upgrade to device running newer version of Palm OS
    - Capability removed in OS >= 5.0
  - Physically prevent access to HotSync port
    - Hardware lock (Ex.: Kensington, Targus, Belkin)
    - Plastic glued into place, permanently disabling port
    - Cutting specific traces on circuit board



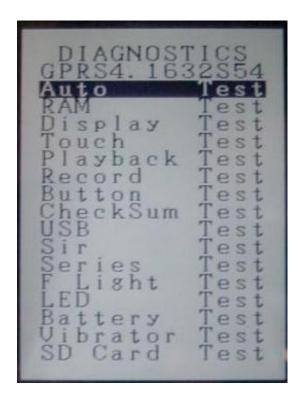
### Visual Studio .Net Debugger

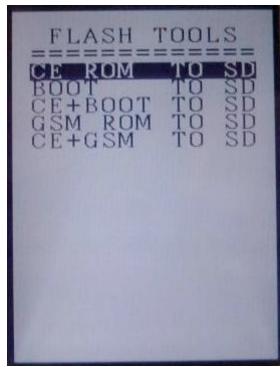
- Exists for debugging during app development
  - Provides remote debugging and device access to Windows CE / Pocket PC
  - Developer's documentation publicly accessible
  - Uses ActiveSync protocol
- Can access Pocket PC registry, install/delete/run apps, export databases

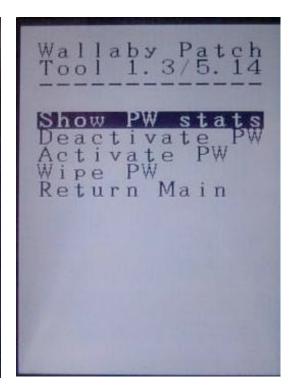
## Pocket PC Phone Edition and XDA Bootloader

- Allows access to a device without passing any access controls
- Provides a detailed debugging and diagnostics interface through sync port
- Special mode to recognize diagnostic external memory cards and can execute code directly from them

## Pocket PC Phone Edition and XDA Bootloader 2







Source: "The Phone in the PDA," Job de Haas, Black Hat Briefings Amsterdam 2003



## **Psion Link Protocol (PLP)**

- Proprietary protocol between device and PC
- Partially reverse-engineered and documented
- Full access to data on all drives (internal and external)
- Can be accessed even if system lock-out is enabled
- Ex.: plp-tools, PDA Seizure (soon)

### **Physical Access to Data**

- Physical attack often more difficult than software attack, but still possible without detection
- Secure hardware design principals not employed
  - Possible to open device and read memory
  - Access data using manufacturing test interfaces (e.g., JTAG)
- Recommendations:
  - Be aware of physical location at all times
  - Store critical data on external memory card and remove when not in use



### **Attack Vectors & Malicious Code**

#### Three stages:

- Infection
- Storage
- Actions
- Anti-virus tools exist
  - Do not protect from many of weaknesses (yet)
  - Install anyway to add another "layer" of security
  - McAfee: By 2005, malicious mobile phone attack will have potential to infect 33% of all users within 3 days



#### Infection

- Application installation procedure
- Desktop conduits
- External memory cards
- Network connectivity
- Wireless communications
- Telephony



### Infection: Application Installation

- Installation procedure for Palm, Pocket PC, and BlackBerry all very simple and similar
  - Palm: Apps to be loaded are copied into /Palm/<user>/Install
  - Pocket PC: Apps to be loaded are copied into directory listed in HKLM\Software\Microsoft\Windows CE Services\InstalledDir
- No confirmation or authentication exists
- Recommendations:
  - Manually check installation directory before synchronization



### Infection: Desktop Conduits

- Enable transfer of data between device and specific desktop application
- Standard conduits exist
  - Palm: HotSync
  - Pocket PC: ActiveSync
  - Psion/EPOC16/EPOC32: PsiWin, plp-tools
- Route data to Personal Information Manager (PIM) or third-party application
  - Microsoft Outlook/Exchange/Office, Netscape, Lotus Notes, etc.

### **Infection: Desktop Conduits 2**

- Possible for cross-architecture transfer
  - Mixing business with pleasure
  - Ex.: Windows PC to/from Pocket PC
- Could exploit a known security problem in the destination desktop app
- Recommendations:
  - Only synchronize your device with a trusted desktop
  - Use anti-virus software on both platforms to scan incoming data before passing it to destination app



### **Infection: External Memory Cards**

- Most all devices have support for external memory cards
  - Ex.: SD, CompactFlash, MemoryStick, SmartMedia
- Some devices will auto-run applications directly from memory card upon insertion
- Pocket PC: AutoRun
  - Will bypass system password protection
  - Copious amounts of documentation on MSDN
- Palm (Sony): MemoryStick Autorun



### **Infection: Network Connectivity**

- Devices with TCP/IP or other network functionality provide additional attack vectors
  - Ex.: Remote attacks against device
  - Ex.: Attacks against network from compromised device
- Pocket PC: ActiveSync listens on Port 5679 for remote connection
  - Can launch Denial of Service by continuously establishing and closing connection



### **Infection: Network Connectivity 2**

- Recommendations:
  - Don't use ActiveSync on an unencrypted/untrusted network
  - Disable all unneeded network connections
    - Ex.: ftpd, telnetd

## Infection: Wireless, IR/IrDA

- Point-to-point, close quarters
- No native authentication
- Viable conduit for propagation with collusion on the receiving end
- Ex: Trick the recipient into accepting a malicious program
- Ex: Beam malicious code in the form of a business card object

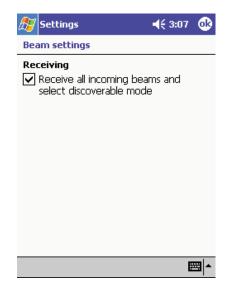


## Infection: Wireless, IR/IrDA 2

- Recommendations:
  - Disable IR port until needed
  - Common sense: Do you trust the other party?
  - Extreme: Do not accept any beamed connections
  - Extreme: Put electrical over the IR port to prevent

rogue connections







## Infection: Wireless, RF

- Suitable for longer-distance communications
- Many different protocols, each with their own security problems
  - Bluetooth, WiFi/802.11b, HomeRF, Mobitex, GPRS
- Ex: Sending malicious e-mail or attachment to the device
  - Buffer overflow or SMS message to intentionally crash device

## Infection: Wireless, RF 2

- Recommendations:
  - Disable wireless functionality until needed
  - Disable all server applications (e.g., web, FTP)
  - Add passwords to Bluetooth services if possible



# Infection: Telephony (SMS/GPRS)

- SMS Attacks
  - Broken UDH caused crash in some Nokia phones
  - Spoofed SMS messages: Originating Address field can be arbitrarily set to anything
  - Ex.: Virus propagated via SMS by resending itself to all phone numbers in the device's address book
- Pocket PC: GPRS connections do not require user confirmation
  - Ex.: Connection can be established programmatically by Trojan horse



# **Storage and Payload Hiding**

- User data areas
- Flash memory

## **Storage: User Data Areas**

- User data and applications stored in RAM
- Malicious code would save program or payload into a standard area
  - Palm: Database
  - Pocket PC: Application Shared Space
- Possible on many portable devices due to lack of protection/access control of data
  - Palm OS 5 has code signing support to ensure that malicious programs cannot tamper with data on device



## **Storage: Flash Memory**

- Flash ROM increasingly being used for OS storage
  - Current devices vulnerable due to no protection or secure hardware mechanisms
- Unused space likely for malicious app storage
  - Anti-virus software does not currently detect access
  - Palm: 128-2424kB free
  - Pocket PC: Many MB free
- Legitimate third-party applications exist to backup data into free areas of Flash
  - Malicious code could use same functionality



## **Actions**

- Flash memory modification
- Register manipulation
- Further attacks or virus propagation

## **Actions: Flash Memory Modification**

- Any data not stored in protected Flash ROM areas is subject to erasure or modification
- Ex: Rewriting OS with Trojan, modifying or destroying critical system data
- Devices provide "boot loader" for OS and Flash upgrades
  - Ex.: XDA, Pocket PC Phone
- Recommendations:
  - Use an older device that stores OS in non-rewritable memory (ROM)

## **Actions: Register Manipulation**

- Lack of layer control allows user apps to directly access hardware via memory mapping
- How to detect with anti-virus software?
  - Hard to distinguish between legitimate and malicious access

Register(s)	Potential Effects
Phase-Locked Loop (PLL) and Power Control	System can be halted
Chip-Select and Addressing	Corrupt memory maps making code and data fetches impossible
LCD Control Module	Affect LCD functionality

# Actions: Further Attacks & Virus Propagation

- Platform could be used as a launch pad for additional attacks or malicious code propagation
- Ex.: Attacker to use device to mask steps
- Ex.: Virus propagated via SMS by resending itself to all phone numbers in the device's address book

#### **General Recommendations**

- Use power-on password and encryption to protect data
  - Adds an additional layer of "security"
  - Many third-party solutions available
    - Ex.: Certicom movianCrypt for Palm and Pocket PC
- Monitor synchronization logs
- Keep up to patch level on all desktop and handheld apps (e.g. Palm Desktop, MS ActiveSync, etc.)

## **General Recommendations 2**

- Make regular backups of mobile device data
- Store critical data on removable memory and keep with you at all times
- Use VPNs on mobile device if possible
- Be aware of:
  - Physical location
  - What critical information you are storing
  - What apps are being installed onto the device



#### **Conclusions**

- Understand the risks and implement recommendations
- Hard, if not impossible, to detect tampering and data theft
- Most products not designed for security
  - Vendors starting to take small steps
  - Understand your threat model
  - Analyze before implementation



### **Conclusions 2**

- Simplistic and common classes of problems
  - No access control
  - Weak user authentication
  - Many avenues for malicious code
- Malicious code propagation is a real threat, though not yet fully realized
  - As mobile device use becomes more widespread, risks become amplified



#### References

- Kingpin, "Palm OS Password Retrieval and Decoding," September 2000, www.grandideastudio.com/files/security/mobile/ palm password decoding advisory.txt
- 2. Hernan Ochoa, "ActiveSync 3.0 Vulnerability: Obtaining the Partnership's Password," www.cegadgets.com/arthernanpass.htm
- 3. Pascal Meunier, et al, "ActiveSync, TCP/IP and 802.11b Wireless Vulnerabilities of WinCE-based PDAs," CERIAS Technical Report 2002-17.
- 4. Kingpin, "Palm OS Password Lockout Bypass," March 2001, www.grandideastudio.com/files/security/mobile/ palm\_backdoor\_debug\_advisory.txt



# Additional Reading: Palm OS

- PalmSource, Palm OS Web Page, www.palmsource.com
- Grand Idea Studio, Mobile Device Security Web Page (pdd, Ointment, NotSync, PalmCrypt, TBA, BeamCrack),
   www.grandideastudio.com/portfolio/index.php?id=1&prod=17
- HandEra, JackFlash, www.handera.com/Products/JackFlash.aspx

## **Additional Reading: Pocket PC**

- Microsoft, Pocket PC Mobile Devices Web Page,
   www.microsoft.com/windowsmobile/default.mspx
- Pocket PC Developer Network, www.pocketpcdn.com
- XDA Developers, www.xda-developers.com
- ITSX Pocket PC Resources, www.itsx.com/pocketpc
- Datalight, FlashFX, www.datalight.com



## **Additional Reading: Forensics**

- Paraben, PDA Seizure, www.paraben-forensics.com/pda.html
- M. Burnette, "Forensic Examination of a BlackBerry Wireless Device," www.rh-law.com/ediscovery/Blackberry.pdf

## **Additional Reading: Wireless**

- William Arbaugh, Wireless Research Web Page, www.cs.umd.edu/~waa/wireless.html
- Ollie Whitehouse, "War Nibbling: Bluetooth Insecurity," October 2003,
   www.atstake.com/research/reports/acrobat/atstake\_war\_nibbling.pdf
- Job de Haas, "SMS Security," 2001, www.itsx.com/hal2001/hal2001itsx.ppt



# Additional Reading: Anti-Virus & Encryption

- F-Secure, Handheld Solutions Web Page, www.f-secure.com/wireless
- Certicom, movianCrypt, www.certicom.com/index.php?action= product,mcrypt

## Thanks!

**Grand Idea Studio, Inc.** 

http://www.grandideastudio.com

joe@grandideastudio.com