The phone in the PDA
Pocket PC Phone edition security

Job de Haas
<job@itsx.com>
Overview

- What is Pocket PC Phone edition.
- Some horror scenario's.
- Features versus flaws.
- Tools of the trade.
PDA Operating Systems

- Palm
  - PalmOS
- Symbian
  - Alliance: Nokia, Sony-Ericsson, Motorola etc.
- Microsoft
  - Pocket PC / Windows CE
Pocket PC

- Windows CE / Embedded
- Version 3.0, 4.x/.NET in the making
- Broader than PDA’s:
  - Automotive
  - Smartphone
- Tuned to small devices with Flash ROM
Pocket PC Phone edition

- Major implementation by HTC
- Strong ARM & TI GSM part
- Multiple brands
Other developments

- Smartphone also made by HTC
- Mainly branded as Orange SPV
- Even buggier than XDA
Internals

- StrongARM 206 Mhz processor running wince 3.0
- TI HERCOM chipset (OMAP predecessor) running Nucleus (with a G23 GSM stack by former Condat AG)
System Circuit Diagram

PDA
- LCD 62Mhz
- 240x120

CPU
- SA 1110 (265Mhz)

BASE-BAND
- ULYSSE (25Mhz)
- Nausica (13MHz)

RF
- (900,1900Mhz)

Memory
- SDRAM/FLASH (10MHz)

Audio
- (22MHz)

POWER
- (1MHz)

CHARGER

May 15th, 2003
The phone in the PDA
Wince part

- The part running wince is very similar to iPAQ (earlier models also by HTC)
- It contains a boot-loader that can be entered by pressing power-on while resetting.
- Communicates with the phone part over a serial line.
HERCOM / OMAP

• Combined ARM & DSP core.
• Provisions for typical phone interfaces such as SIM card.
• Stand-alone from the Pocket PC processor.
General impression

• The product as a whole is immature. (hey, what’s new?)

• Pocket PC and the apps added for the phone edition show a complete lack of understanding of phone usage:
  – Names are not shown on incoming SMS.
  – The phone cannot directly be used as a modem.
  – Software running on the device is severely limited by TAPI (FAX software is not supported)
Horror scenario’s

- User is CEO in board meeting.
- Attacker sends SMS/MMS with payload.
- Payload turns on GPRS and retrieves main payload.
- Main payload starts recording the microphone and sends it over Internet.
- Payload shuts down display so the device appears turned off.
Horror scenario’s

- Corporate user run’s infected application.
- Application stays dormant until active sync.
- Application connects over GPRS to attacker
- Backdoor path into corporate network is created.
Pocket PC security features

- Password-on-wake-up.
- ‘Admin’ policy to prevent installation of executables.
- Hooks for virus checking applications.
- Code signing / installation limitations.
Pocket PC typical security flaws

- All applications run in ‘Administrator’ context. ie. Can access all memory. (for XDA)
- No integrated concept with phone: eg. phone PIN readable from registry.
- ‘Non executable protection’ can be circumvented by custom apps.
Unlocking

• Is what phone hacking is currently mostly about.

• Although Phone memory is only indirectly reachable, research is possible through:
  – ROM image in upgrades.
  – AT commands that give access to memory.
  – Run code in GSM RAM through upgrade process.

• Unlock code is directly readable from GSM ROM:
  – AT%UREG?3FE00C,4
XDA-Manipulator

• A tool that manipulates several GSM parameters through a serial cable.
• Can make a GSM memory dump.
• Is available from:
  http://www.xda-developers.com
XDA-Manipulator

XDA-developers.com presents the:

XDA manipulator

Status: Ready
SID lock: 02345288
GID lock: <none>
IMEI: 350312010043185

Keep first 8 digits the same

Call timers: <non-zero>

reset  Help
ARM reversing

- Fairly straightforward instruction set.
- IDA Pro support.
- Free embedded development tools from Microsoft allow remote debugging.
- Linux was ported to iPAQ:
  - Internal knowledge
  - Cross compiling toolchains
Future outlook

- Wince .NET
  - More attention to security features.
  - Still not tuned to real live use.
- Problems of the desktop move to PDA.
- Embedded systems increase the unjustified feeling it will be ‘hard’ to break in to them.
- More and more developing for embedded systems becomes ‘easy’.

⇒ increase bad apps, increase attackers.
Resources

• At time of printing the list of resources was not complete, but it can be found at

http://www.itsx.com/pocketpc