Windows CE Hardening
Black Hat 2003
Your Speaker

• Josh Daymont is the CTO at MobileSecure, Inc.
• Security research resulted in a number of published advisories
• A leading Windows CE security expert
• Co-created the ISS X-Force
Agenda

• Overview of Windows CE Security
  – Assets, Threats, and Vulns
• Uses for Windows CE
• Security in different environments
• Building a Secure WinCE OS
• Introduction to Hardening PocketPC 2002
• Q&A
Overview

• The Assets
  – Privileged access to the device
  – Routine access to the device
    • Device data
  – Network resources
  – Peripherals such as a cellphone, modem, industrial tool, or bluetooth device
Overview

• The Threats
  – Worms
  – Malicious groups or individuals
  – Viruses
  – Spammers
The Vulnerabilities

• Includes existing vulnerability types
  – Malformed packet attacks
  – Buffer overflows & format string attacks
  – Resource consumption and DOS
  – Web application and browser attacks
  – Authentication spoofing & session hijacking
  – Traditional wireless attacks
    • Interception
    • Jamming
The Vulnerabilities

• **Windows CE introduces new attacks**
  – Flash attacks
  – Reset attacks & other hardware specific problems
  – Lack of a security subsystem enables universal user spoofing
  – Kernel privilege escalation
  – Personal area network (PAN) vulnerabilities
  – Telephony attacks (SMS, GPRS)
Uses for Windows CE

- PDAs
- “Smartphones”
- Home Appliances (Wash/Dryer etc)
- Ultra small servers
- Surveillance equipment
- Automobile control systems
Security Requirements
PDAs & SmartPhones

• Additional requirements include security for attached telephony hardware.
• Bluetooth services must have passwords
• Disable infrared file transmission
• Only synchronize your device with a trusted desktop
• Use network security software if possible
• VPNs are important for mobile devices
Servers

- Windows CE supports a number of server applications
  - IIS for CE
  - SQL Server for CE 2.0
- A resident intrusion prevention system is a must
• Basic Authentication allows multiple users but only one global password
  – Do not use basic authentication
• NTLM Authentication allows domain passwords
  – Perform domain authentication only over a VPN
• WinCE is built using Platform Builder from Microsoft

• Several CE components should be examined carefully by CE OEM customers
  – ActiveSync
  – Internet Browser
  – Bluetooth and IRDA
  – “Trusted Environment”
• **Components continued**
  – TCP/IP
  – Filesystems
  – MSMQ
  – IIS
  – SNMP
  – SQLServer
  – FTPd & Telnetd
• ActiveSync is used to automatically transfer files from a device to a server
  – over a direct physical link
  – over the internet
• No confidentiality of transferred data
• Authentication depends on screen-lock password
  – Can be brute forced
  – Man in the middle attack possible
• Use PIE rather than traditional IE
• PIE’s reduced functionality will limit exposure to new vulnerabilities
• Consider removing VBScript
• Keep browser enabled ActiveX controls to an absolute minimum
• Both these modules rely on OBEX
• Always turn off automatic receives
• Ensure Bluetooth uses passwords
  – Bluetooth passwords may not hold out against a determined attacker
• IRDA has no native authentication
• The trusted environment allows the WinCE kernel to restrict what code is allowed to run based on an OEM supplied function.
• The trusted environment can be circumvented if not implemented correctly.
• The key weakness of the trusted environment lies in the ability of user code to execute within the context of the kernel.
• For now, always assume anything running in usermode has complete access to kernel memory – Disable Full Kernel Mode!
• Be sure to disable IP routing by default

• What networks will the device communicate over
  – Cellular/GPRS & PPP
  – WiFi (802.11) & Ethernet (802.3)
    • Force as much encryption as possible
Building a Secure WinCE OS – Filesystems

- Consider adding rudimentary file ACLs to your OS if needed
  - Based on application accessing as opposed to user
- Consider adding encryption here
  - Alternative would be through a 3rd party application
• The MSMQ management ISAPI extension should be disabled for devices with IIS
  – Be very careful about leaving this in
• MSMQ is a large heavyweight system of the type that typically breeds vulnerabilities
  – Ask yourself if you really need MSMQ on a particular device
Building a Secure WinCE OS – IIS

- WinCE typically uses IIS for remote administration or status display
  - This can be dangerous especially because
    - WinCE lacks many native security features that IIS traditionally relies on
    - WinCE may operate over hostile wireless networks that allow increased opportunities for sniffing and man in the middle
- IIS should operate only over SSL for almost all applications
Building a Secure WinCE OS – IIS

- Avoid NTLM authentication over wireless
- For basic authentication everyone has the same password!
- Make virtual directory access controls as restricted as possible
- Treat IIS usernames as though they were passwords
  - Never store a username outside the registry
  - Restrict non-administrator usernames to view only and no scripting
• This protection exists only for IIS and the underlying files themselves are unprotected

• Other ways to access files
  – Physical access
  – Faulty server side code
• Best practice: Never use SNMP
• If you must
  – Use very hard to guess community names
  – Try to never give anyone write access
  – Turn authentication traps on
  – Always use the “PermittedManagers” registry setting
Building a Secure WinCE OS – SQL Server

- SQL Server for CE has no network logins
  - Can use replication
  - Can use Remote Data Access (RDA)
- Almost always used with IIS
- SQL Injection still applies
- Consider the sensitivity of the data stored
  - Is the device physically secure?
• Never use FTPd if you need security
  – Implement something yourself instead
• FTPd authentication options are similar to IIS
  – Except no encryption
• Limited file security for anonymous logins
  – Anonymous access should always be disabled anyway
• Telnetd provides less security than Ftpd
  – No encryption
  – Similar authentication
  – No access controls
  – No “chrooting”
Building a Secure WinCE OS – Summary

- Microsoft has delegated to responsibility for WinCE security to the OEM customer
  - OEMs must include security professionals in the OS design and implementation process
  - Most OEMs seem to be skipping security within CE as of today
- It is impossible to build a secure WinCE OS “out of the box”
• For Windows CE users who license a production copy of CE from an OEM customer
• How to harden depends significantly on what the OEM has provided
• This section is geared primarily towards PocketPC 2002
How to Harden CE: General

- NEVER use ActiveSync over an unencrypted network
- Do not accept beamed documents
  - Start -> Settings -> Connections -> Beam
- Use a VPN whenever possible
- Enable the PIN for any cellular telephone
  - Start -> Settings -> Personal -> Phone
- Make regular backups
  - If you don’t have backup software pre-installed you can purchase a solution for $10
How to Harden CE: Authentication

• Require a logon password
  – Start -> Settings -> Password
  – Change to prompt period from 1 hour to something around 5 minutes
  – Password will be required for synchronization
  – Use improved password protection such as that available from MobileGuard whenever possible

• Use a PocketPC security solution such as MobileGuard™ for increased password security

• Beware: check device lockout period

• Password stored in registry key as a hash
How to Harden CE: Authentication

• PPP passwords used on the device are stored in plaintext registry entries
  – Consider the risks before storing internet passwords
Exploit Example

- IE Exploit
- Sample Backdoors
Summary & Conclusions

• Windows CE is a useful and feature rich solution for embedded or mobile devices
• Security is still a concern but the problem can be solved
• Pay special attention to the environment in which the device will be operated
• The material discussed in this presentation can be covered in detail through a MobileSecure consulting engagement
Q&A

joshd@mobile-secure.com