Microsoft

Creating a More Secure Device with Windows Embedded Compact 7

Douglas Boling

Boling Consulting Inc.

Windows Embedded Compact 7

About Douglas Boling

- Independent consultant specializing in Windows Mobile and Windows Embedded Compact (Windows CE)
  - On-Site Instruction
  - Consulting and Development
- Author
  - Programming Embedded Windows CE
    - Fourth Edition

Agenda

- Security Holes
- WEC Security
- Basic Practices
- More secure

Security Holes

- Full function shells
- Debugging tools
- Extra driver functionality
- Other components

Remove Shells

- Explorer Shell
  - Very useful for debugging
  - Bad to see it displayed when an unexpected error terminates application
  - Control panel applets can change basic behavior

- Beware of “Win Key” combinations
  - Even if your keyboard doesn’t have a windows key, keyboards can be attached

A Proper Shell

- Create your own shell
  - Base it on MINSHELL
  - C:\WINCE700\public\wceshellfe\oak\taskman
- Minshell
  - Provides desktop and hidden ‘taskbar’ window
  - Can launch and kill applications
  - Intercepts proper system keys
- Modify Minshell to remove the pop-up dialog that switches/kills applications
  - Add features you may want… like a auto-restart thread

Remove Debugging Components

- Telnet server
  - Useful for debugging
  - Not designed as secure server
- FTP server
  - Useful for debugging
  - Not designed as secure server
- Bootloader download capability
  - There is no such thing as a “secret” key combination

Remove Unnecessary USB Client Drivers

- Unless required, remove USB HID driver
  - Unexpected keyboards and mice can change behavior
- USB Storage device driver
  - Method of introducing code into system
  - Method of removing data from the system
- It is possible to configure registry to limit client drivers to load only for specific hardware

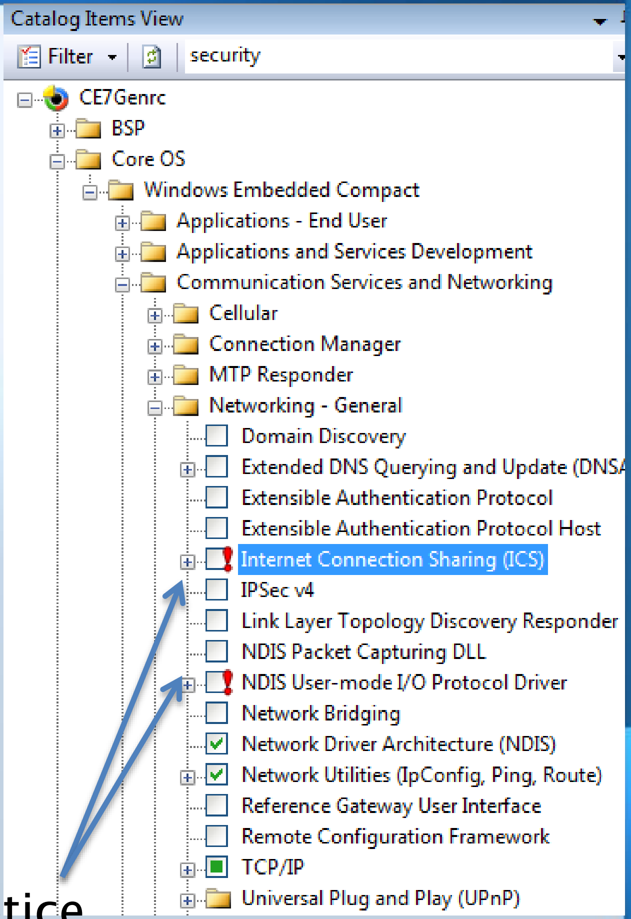
Remove Unnecessary Components

- It’s easy to simply to use a large image so app devs don’t have to worry about compatibly
  - Easy solution that has consequences

- More components mean a larger attack surface
  - Just say no… to extra components

Insecure Components

- The nature of Embedded systems means that there are inherently insecure components that can optionally be used in WEC 7
  - User Mode Network configuration driver
- Platform Builder warns the developer when these components are included in the build
  - Balance need vs. exposure



Catalog Items View

Filter | security

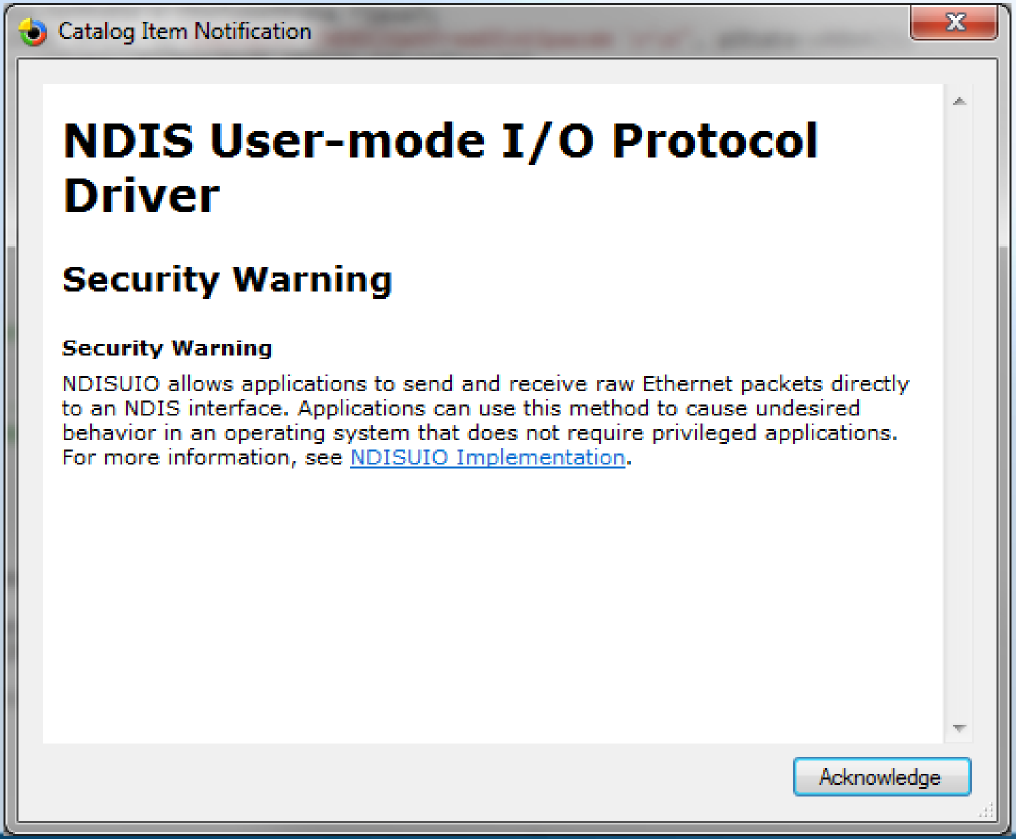
- CE7Genrc
  - BSP
  - Core OS
    - Windows Embedded Compact
      - Applications - End User
      - Applications and Services Development
      - Communication Services and Networking
        - Cellular
        - Connection Manager
        - MTP Responder
        - Networking - General
          - □ Domain Discovery
          - □ Extended DNS Querying and Update (DNSA
          - □ Extensible Authentication Protocol
          - □ Extensible Authentication Protocol Host
          - □ ! Internet Connection Sharing (ICS)
          - □ IPSec v4
          - □ Link Layer Topology Discovery Responder
          - □ NDIS Packet Capturing DLL
          - □ ! NDIS User-mode I/O Protocol Driver
          - □ Network Bridging
          - ☑ Network Driver Architecture (NDIS)
          - ☑ Network Utilities (IpConfig, Ping, Route)
          - □ Reference Gateway User Interface
          - □ Remote Configuration Framework
          - ■ TCP/IP
          - Universal Plug and Play (UPnP)

Warning notice

Windows Embedded Compact 7

Warning Dialog Example

- From User Mode network I/O driver



NDIS User-mode I/O Protocol Driver

Security Warning

Security Warning

NDISUIO allows applications to send and receive raw Ethernet packets directly to an NDIS interface. Applications can use this method to cause undesired behavior in an operating system that does not require privileged applications. For more information, see NDISUIO Implementation.

Windows Embedded Compact 7

WEC 7 Kernel Security Features

Address Space Randomization (ASR)

- Randomizes load address of DLLs
  - Increases security by making addresses nondeterministic
- Enable with environment variable
  - IMGSSLRENABLE=1

```
; Address Space Layout Randomization:
;  0 = disabled
;  non-zero = enabled
IF IMGASLRENABLE
[HKEY_LOCAL_MACHINE\init\BootVars]
               "AslrEnabled"=dword:1
ENDIF IMGASLRENABLE
```

Data Execution Prevention (DEP)

- Prevents code from executing out of data pages
  - Supported on ARMv6 and later architectures only
  - Not x86
- Can be configured to support entire system or by application
  - Entire system has “No Execute” flag set for data pages
    - All applications must be marked as NX aware in PE header
  - Only selected applications have “No Execute” flag set
    - These applications have NX aware bit set in PE header
- Regardless, NX bit always set for kernel data pages

Enabling Data Execution Prevention

- Set environment variable
  - IMGNXSUPPORT=1

- Configure registry variable to determine level if DEP

```
; Enable No eXecute support (Data Execution Prevention)
;   0 = no NX support at all
;   1 = by application NX support (NX support by PE flags)
;   2 = NX flag enforced (only load NX compatible executables)
; If IMGNXSUPPORT is set, we default to by application NX support.
IF IMGNXSUPPORT
[HKEY_LOCAL_MACHINE\init\BootVars]
  "NXSupport"=dword:1 ; honor nxcompat flag
ENDIF IMGNXSUPPORT
```

- Marking application as DEP compatible
  - In SOURCES file, add the line DEP_COMPATIBLE=1

Application Security

Basic Practices

- Secure CRT
  - Use the safe string functions instead of the standard CRT functions
  - The latest CRT nags you into doing just this
- For backward compatibility do the following

```
// Necessary because CE5 doesn't have safestring lib.
#if _WIN32_WCE<0x600
#define wcscpy_s(a,b,c)  wcscpy(a,c);
#define wcscat_s(a,b,c)  wcscat(a,c);
#endif
```

Use Windows Imaging Component

- WIC API replaces the old Imaging component
  - More secure
- Will be the future API
  - Might as well convert now
- Look for documentation on line
  - Check the Windows 7 documentation
    - The WEC 7 docs don’t have WIC included

Cryptography, Next Generation (CNG) API

- Windows Embedded Compact 7 supports extensible cryptographic API
  - Same API as the desktop
- Allows extensible set of encryption providers
  - APIs to enumerate providers, select specific/default providers
- ENCFilter sample in CE 6 provides example of using CryptoAPI
  - Removed from WEC 7
  - Should be fairly easy to port forward

Load Verification

- Load verification verifies modules as they are loaded
  - Verifier makes a load / no-load decision
  - By default, all modules in .bin file are considered trusted
- User definable DLL can vet a module as it is loaded
  - Microsoft provides a verifier that looks for embedded certificates
  - Loaded by kernel on boot
- LVMod API documented
  - This allows OEMs to replace module with own validation scheme

Anti-Security

- Sometimes its better to be faster than more secure
- WEC 7 copies all buffers when moving from user to kernel
  - This slows down calls to the OS
- To speed up, move time critical code to kernel mode driver
  - Code that is highly interactive with API

Summary

- Security is basic common sense
  - But you need to actually consider it
- Right-size your image
  - Explorer
  - Telnet
  - FTP
- Crypto functionality quite good if you need it
- Balance security need with performance requirements

Questions…

Doug Boling

Boling Consulting Inc.

www.bolingconsulting.com

dboling @ bolingconsulting.com