

# **Hands-On Ethical Hacking and Network Defense Second Edition**

## *Chapter 9*

### *Embedded Operating Systems: The Hidden Threat*

# Objectives

- After reading this chapter and completing the exercises, you will be able to:
  - Explain what embedded operating systems are and where they're used
  - Describe Windows and other embedded operating systems
  - Identify vulnerabilities of embedded operating systems and best practices for protecting them

# Introduction to Embedded Operating Systems

# Introduction to Embedded Operating Systems

- Embedded system
  - Any computer system that isn't a general-purpose PC or server
    - GPSs and ATMs
    - Electronic consumer and industrial items
- Embedded operating system (OS)
  - Small program developed for embedded systems
    - Stripped-down version of OS commonly used on general-purpose computers
    - Designed to be small and efficient

# Introduction to Embedded Operating Systems (cont'd.)

- Real-time operating system (RTOS)
  - Typically used in devices such as programmable thermostats, appliance controls, and spacecraft
- Corporate buildings
  - May have many embedded systems
    - Firewalls, switches, routers, Web-filtering appliances, network attached storage devices, etc.
- Embedded systems
  - Are in all networks
  - Perform essential functions
    - Route network traffic; block suspicious packets

# Windows and Other Embedded Operating Systems

- Recycling common code and reusing technologies
  - Sound software engineering practices
  - Also introduce common points of failure
    - Viruses, worms, Trojans, and other attack vectors
- Windows and Linux vulnerabilities
  - Might also exist in embedded version
- Windows CE
  - Some source code is available to the public
    - Code sharing is not common
    - Microsoft believed it would increase adoptions

# Windows and Other Embedded Operating Systems (cont'd.)

- Windows Embedded Standard
  - Provides full Windows API
  - Performs many of the same tasks as desktop version
  - Designed for more advanced devices
    - Complex hardware requirements
  - Modular OS
    - Unneeded features can be removed
  - See link Ch 9a

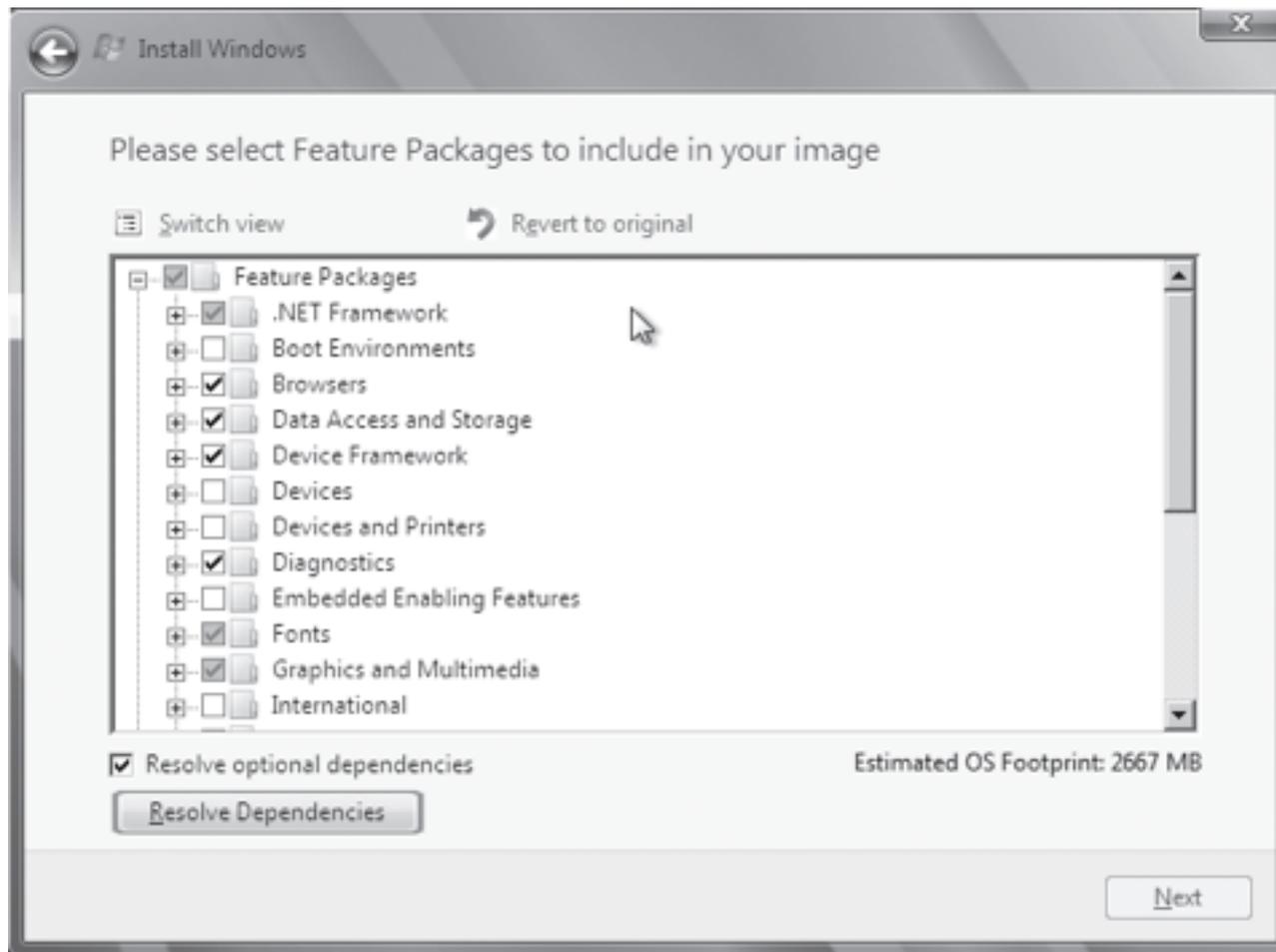


Figure 9-1 Selecting features in Windows Embedded Standard

# Windows and Other Embedded Operating Systems (cont'd.)

- Windows Embedded Standard, code-named Quebec
  - Based on Windows 7
- Windows Embedded Enterprise
  - Embedded versions of Windows Enterprise OSs (e.g., XP Professional, Windows Vista Business and Ultimate, and Windows 7 Ultimate and Professional)
    - Functional versions of Windows desktop OSs
    - Higher hardware requirements

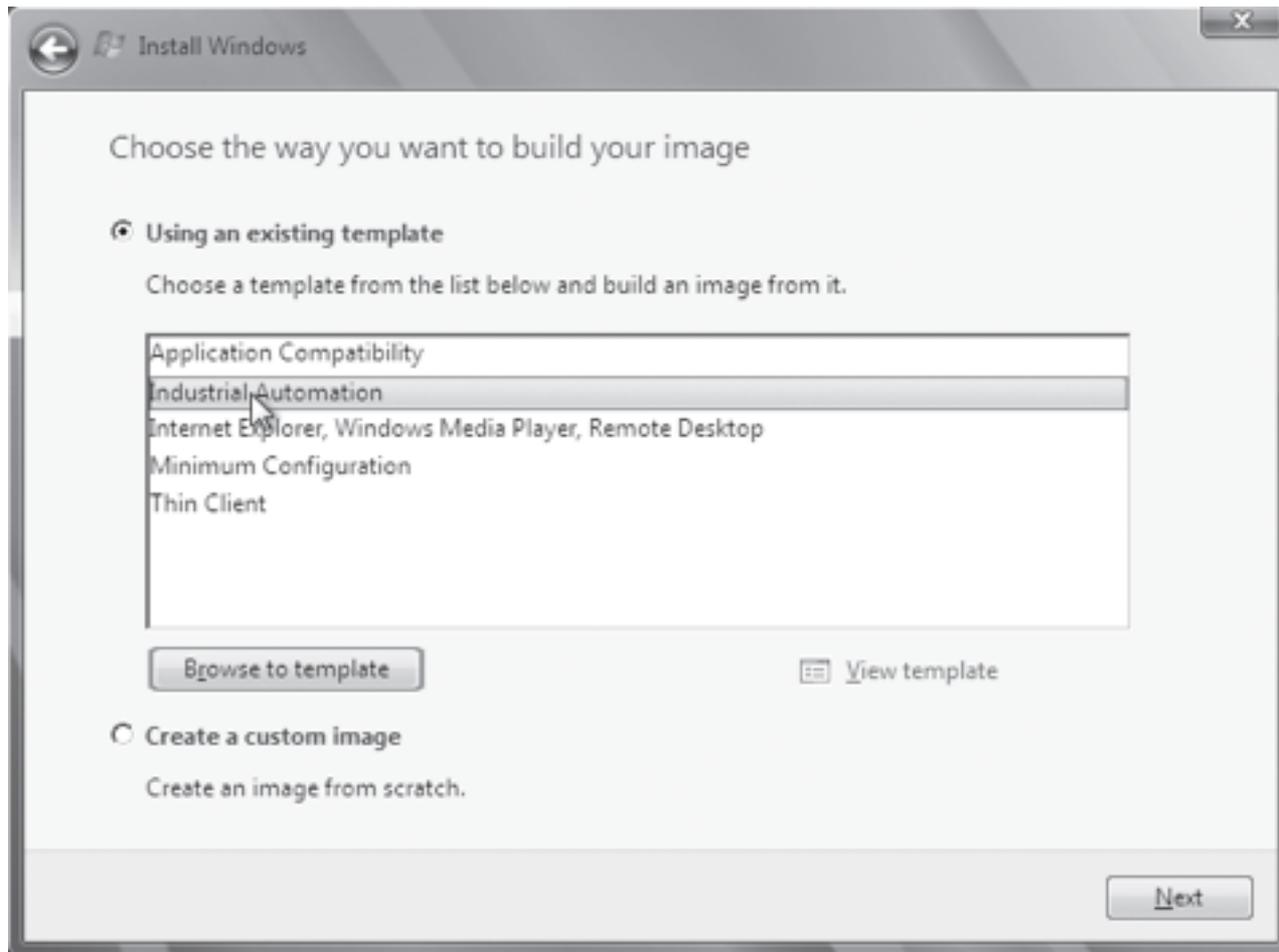


Figure 9-2 Selecting a template for industrial automation

# Other Proprietary Embedded OSs

- VxWorks
  - Widely used embedded OS
    - Developed by Wind River Systems
  - Used in many different environments and applications
  - Designed to run efficiently on minimal hardware
  - Used by a variety of systems



# Other Proprietary Embedded OSs (cont'd.)

- Green Hill Software embedded OSs
  - F-35 Joint Strike Fighter
  - Multiple independent levels of security/safety (MILS)
    - OS certified to run multiple levels of classification
  - Embedded OS code
    - Used in printers, routers, switches, etc.
- QNX Software Systems QNX
  - Commercial RTOS
    - Used in Cisco's ultra-high-availability routers and Logitech universal remotes

# Other Proprietary Embedded OSs (cont'd.)

- Real-Time Executive for Multiprocessor Systems (RTEMS)
  - Open-source embedded OS
  - Used in space systems
    - Supports processors designed to operate in space
- Using multiple embedded OSs
  - Increases attack surface

# \*Nix Embedded OSs

- Embedded Linux
  - Monolithic OS
    - Used in industrial, medical, and consumer items
  - Can be tailored for devices with limited memory or hard drive capacity
  - Supports widest variety of hardware
  - Allows adding features
    - Dynamic kernel modules

# \*Nix Embedded OSs (cont'd.)

- Real Time Linux (RTLinux)
  - OS microkernel extension
  - Turns “regular” Linux into an RTOS
    - Suitable for embedded applications requiring a guaranteed response in a predictable manner
- Linux OpenWrt \* dd-wrt
  - Embedded Linux OS
  - Used in Linksys WRT54G wireless router
    - Found in home offices and small businesses
    - Links Ch 9t, 9u



Figure 9-5 Monitoring bandwidth use with dd-wrt



OpenWrt - Software - LuCI - Iceweasel

OpenWrt - Software ... x

192.168.1.1/cgi-bin/luci;stok=4267f5bc7ae8ac0aaf461c16d9dez

Most Visited Offensive Security Kali Linux Kali Docs Kali Tools Exploit-DB Aircrack-ng Hook Me!

### OpenWrt

Status System Network Logout

<a href="#">Install</a>	luci-l18n-openvpn-vi	git-16.018.33482-3201903-1	5987	Translation for luci-app-openvpn - Tiếng Việt (Vietnamese)
<a href="#">Install</a>	luci-l18n-openvpn-zh-cn	git-16.018.33482-3201903-1	6175	Translation for luci-app-openvpn - 普通话 (Chinese)
<a href="#">Install</a>	luci-l18n-openvpn-zh-tw	git-16.018.33482-3201903-1	1171	Translation for luci-app-openvpn - 臺灣華語 (Taiwanese)
<a href="#">Install</a>	openvpn-easy-rsa	2013-01-30-2	10958	Simple shell scripts to manage a Certificate Authority
<a href="#">Install</a>	openvpn-nossl	2.3.6-5	86753	Open source VPN solution using plaintext (no SSL)
<a href="#">Install</a>	openvpn-openssl	2.3.6-5	171709	Open source VPN solution using OpenSSL
<a href="#">Install</a>	openvpn-polarssl	2.3.6-5	167380	Open source VPN solution using PolarSSL
<a href="#">Install</a>	tayga	0.9.2-2	18865	TAYGA is an out-of-kernel stateless NAT64 implementation for Linux. It uses the TUN driver to exchange packets with the kernel, which is the same driver used by OpenVPN and QEMU/KVM.

Powered by LuCI 15.05-149-g0d8bbd2 Release (git-15.363.78009-956be55) / OpenWrt Chaos Calmer 15.05.1

root@kali: ~#

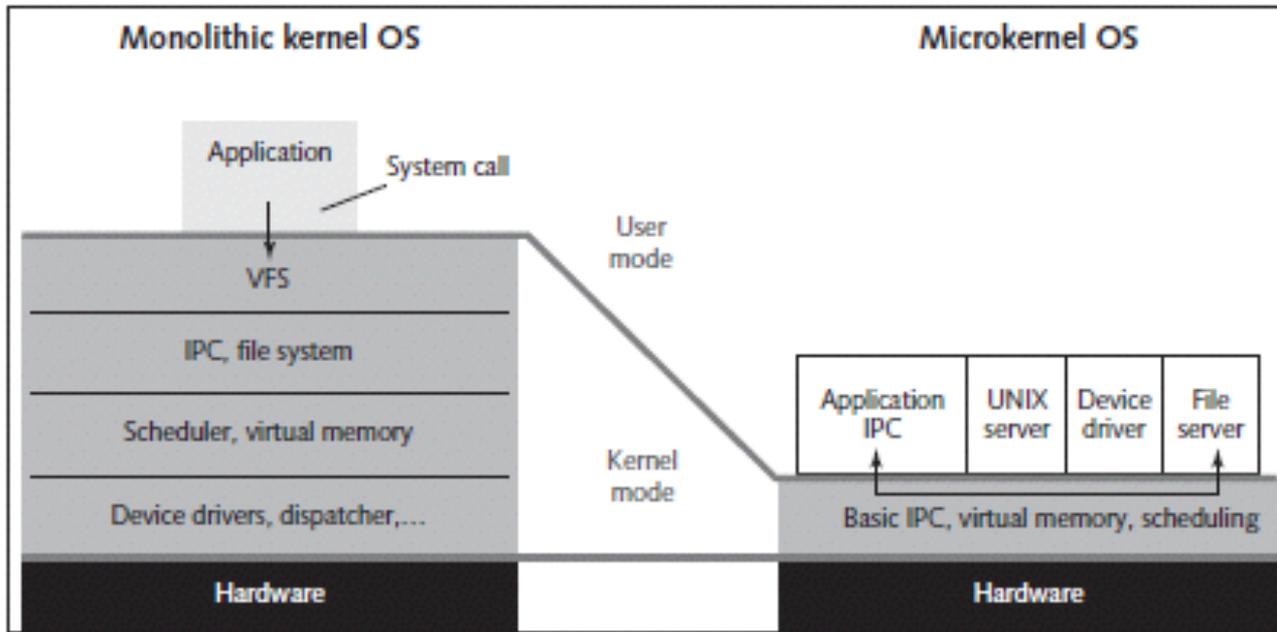


Figure 9-4 Monolithic kernel versus microkernel OSs

# Vulnerabilities of Embedded OSs

# PsyBot

TODAY @ PCWORLD

## Nasty New Worm Targets Home Routers, Cable Modems

Ian Paul, PCWorld Mar 25, 2009 8:30 am



Graphic: Diego Aguirre

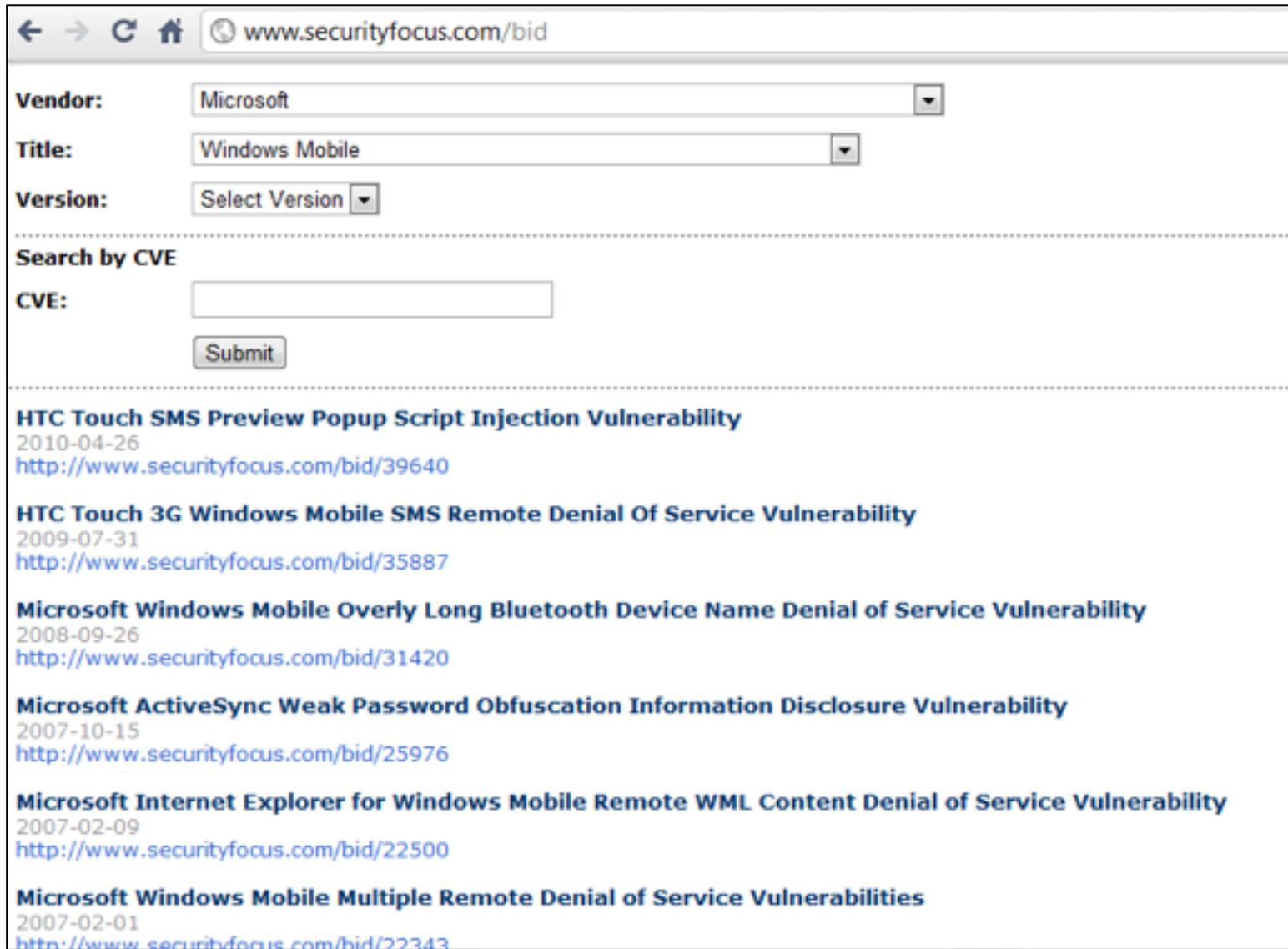
A computer worm has been discovered that can infect 55 different home-based routers and DSL/cable modems including common brands like Linksys and Netgear.

Believed to have originated in Australia and known as "psyb0t" or Bluepill, this is the first worm known to be able to infect residential routers and modems.

Psyb0t is armed with 6000 common usernames and 13,000 popular passwords that it tries in various combinations to gain entry to your home network. Most home-

- Links Ch 9e, 9f

# Windows Mobile Vulnerabilities



The screenshot shows a web browser window with the address bar displaying [www.securityfocus.com/bid](http://www.securityfocus.com/bid). The page contains a search form with the following fields:

- Vendor:** A dropdown menu with "Microsoft" selected.
- Title:** A dropdown menu with "Windows Mobile" selected.
- Version:** A dropdown menu with "Select Version" selected.

Below the search form, there is a section titled "Search by CVE" with a text input field for "CVE:" and a "Submit" button.

The main content area lists several vulnerabilities:

- HTC Touch SMS Preview Popup Script Injection Vulnerability**  
2010-04-26  
<http://www.securityfocus.com/bid/39640>
- HTC Touch 3G Windows Mobile SMS Remote Denial Of Service Vulnerability**  
2009-07-31  
<http://www.securityfocus.com/bid/35887>
- Microsoft Windows Mobile Overly Long Bluetooth Device Name Denial of Service Vulnerability**  
2008-09-26  
<http://www.securityfocus.com/bid/31420>
- Microsoft ActiveSync Weak Password Obfuscation Information Disclosure Vulnerability**  
2007-10-15  
<http://www.securityfocus.com/bid/25976>
- Microsoft Internet Explorer for Windows Mobile Remote WML Content Denial of Service Vulnerability**  
2007-02-09  
<http://www.securityfocus.com/bid/22500>
- Microsoft Windows Mobile Multiple Remote Denial of Service Vulnerabilities**  
2007-02-01  
<http://www.securityfocus.com/bid/22343>

# Vulnerabilities of Embedded OS's

- Impact of attacks have become more serious
  - Embedded OSs are no exception
- Easiest way to profit from hacking
  - Attack devices that store and dispense cash (e.g., ATMs)
    - Involves use of card skimmers or stealing the machines

# Embedded OSs Are Everywhere

- Embedded systems with Y2K software flaw
  - Billions located everywhere
- Today
  - Many more embedded devices
    - Under attack from hackers and terrorists
    - Attackers want to further financial or political causes
  - Addressing security early in design phase is essential

# Embedded OSs Are Networked

- Advantages of connecting to a network
  - Efficiency and economy
  - Ability to manage and share services
    - Keeps human resources and expertise minimal
    - Reduces costs
- Any device added to a network infrastructure
  - Increases potential for security problems

# Embedded OSs Are Difficult to Patch

- General-purpose desktop OSs
  - Simple to patch
    - Wait for vulnerability to be identified
    - Download and install patch
- Embedded OSs
  - Must continue operating regardless of threat
  - Lack familiar interfaces
  - Buffer overflow attacks might be successful
    - Few updates released to correct vulnerabilities
    - Manufacturers typically prefer system upgrades

# Embedded OSs Are Difficult to Patch (cont'd.)

- Open-source software
  - Cost of developing and patching shared by open-source community
- Patching Linux kernel
  - Estimated at tens of billions of dollars
    - Total cost of developing and patching it, in programmer hours
  - Offers flexibility and support
    - Large; has many code portions
- Fixing a vulnerability
  - Weigh cost of fixing against importance of information the embedded system controls

# Hacking Pacemakers

## Defcon: Excuse me while I turn off your pacemaker

August 8, 2008 | [Dean Takahashi](#)

[Comments](#) 



The **Defcon** conference is the wild and woolly version of **Black Hat** for the unwashed masses of hackers. It always has its share of unusual hacks. The oddest so far is a collaborative academic effort where medical device security researchers have figured out how to turn off someone's pacemaker via remote control. They previously **disclosed the paper** at a conference in May. But the larger point of the vulnerability of all wirelessly-controlled medical devices remains a hot topic here at the show in Las Vegas.

Let's not have a collective heart attack, at least not yet. The people on the right side of the security fence are the ones who have figured this out so far. But this has very serious implications for the 2.6 million people who had pacemakers installed from 1990 to 2002 (the stats available from the researchers). It also presents product liability problems for the five companies that make pace makers.

- Link Ch 9g

# Embedded OSs Are in Networking Devices

- Networking devices
  - Usually have software and hardware designed to transmit information across networks
- General-purpose computers
  - Originally performed routing and switching
    - High-speed networks now use specialized hardware and embedded OSs
- Attacks that compromise a router
  - Can give complete access to network resources
    - Attackers follow usual methods of footprinting, scanning, and enumerating the target

# Embedded OSs Are in Networking Devices (cont'd.)

- Authentication bypass vulnerability
  - Common vulnerability of routers
  - Specially crafted URL bypasses normal authentication mechanism
- Router Hacking Contest
  - Link Ch 8h
- After bypassing authentication
  - Attackers can launch other network attacks
    - Use access gained through compromised router

# Reverse Engineering a D-Link Backdoor

By Craig | October 12, 2013 | Embedded Systems, Security

- "...if your browser's user agent string is "xmlset\_roodkcableoj28840ybtide" (no quotes), you can access the web interface without any authentication and view/change the device settings..."
- Link Ch 9s

- DIR-100
- DIR-120
- DI-624S
- DI-524UP
- DI-604S
- DI-604UP
- DI-604+
- TM-G5240

# Embedded OSs Are in Network Peripherals

- Common peripheral devices:
  - Printers, scanners, copiers, and fax devices
- Multifunction devices (MFDs)
  - Perform more than one function
    - Rarely scanned for vulnerabilities or configured for security
  - Have embedded OSs with sensitive information
    - Information susceptible to theft and modification
    - Attackers may use malware or insert malicious links
    - Social-engineering techniques may be used to gain access

# Hacking into a Printer



- Taking control of a printer gives you
  - Access to stored print jobs
  - You can use the printer as a gateway into a secure LAN
    - See link Ch 9i
  - You could also alter the messages the printer produces to send malicious links to desktops

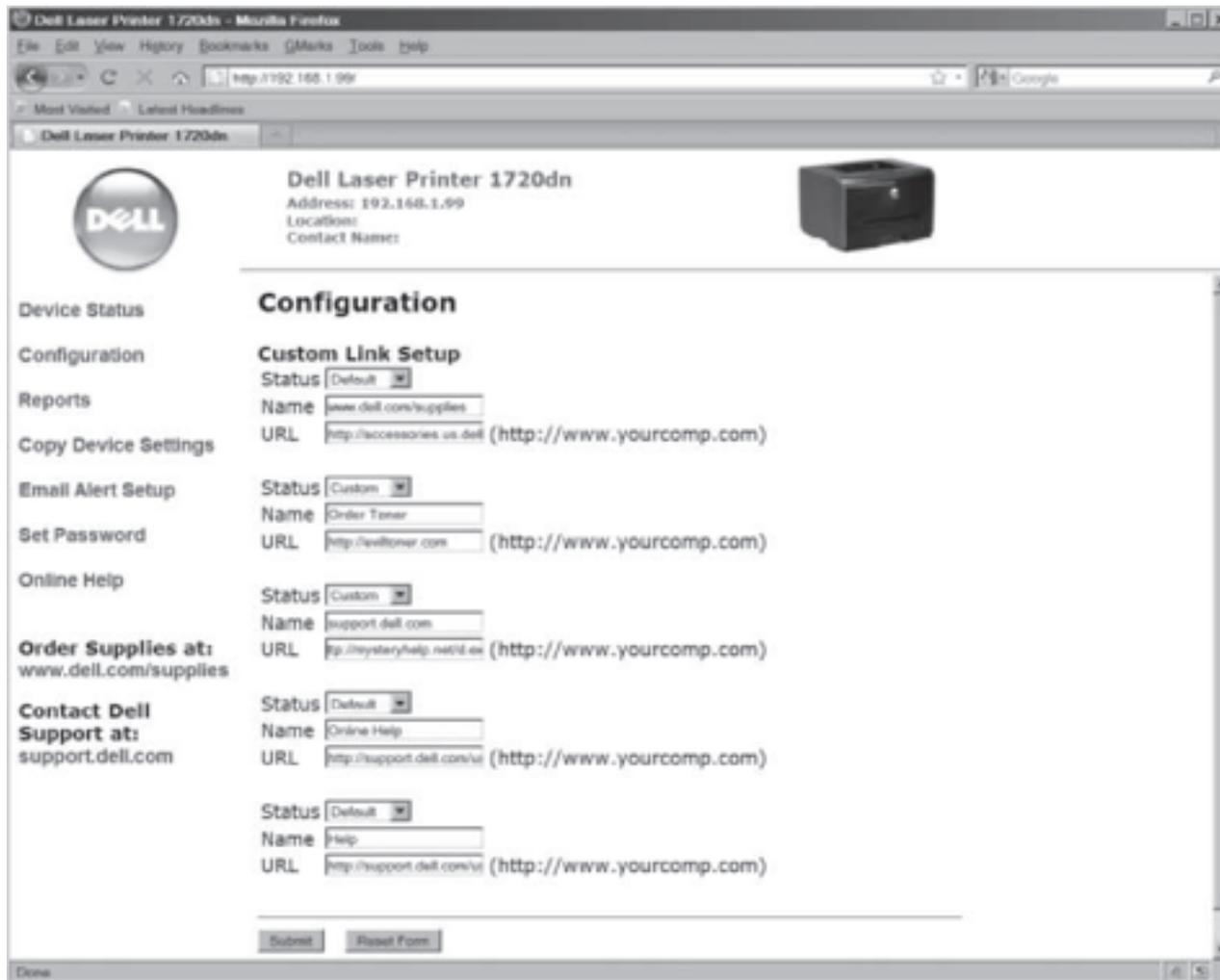


Figure 9-6 Setting up custom links on a Dell networked printer

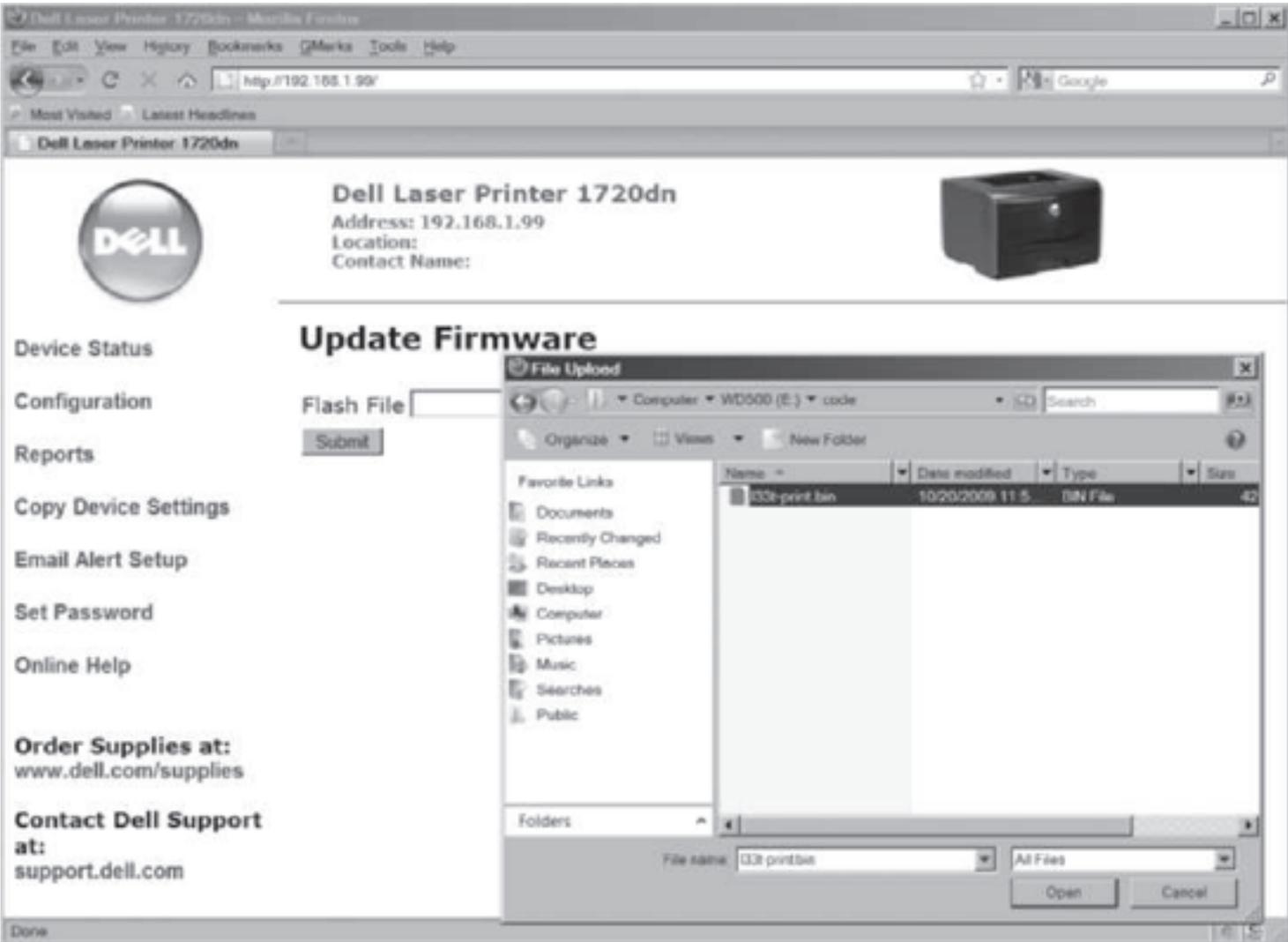


Figure 9-7 Modified firmware being uploaded to a networked printer

# Supervisory Control and Data Acquisition Systems

- Used for equipment monitoring in large industries (e.g., public works and utilities)
  - Anywhere automation is critical
- May have many embedded systems as components
  - Vulnerable through data fed in and out or embedded OSs
- Systems controlling critical infrastructure
  - Usually separated from Internet by “air gap”
    - *Maybe NOT! New info 2 slides ahead!*

# Project AURORA



- In a 2007 security test, a simulated cyber attack on a diesel generator destroyed it
  - Link Ch 9j

# Stuxnet

**Iran confirms massive Stuxnet infection of industrial systems**

Nation's atomic energy experts met last week to discuss ways to eradicate worm, say reports

By Gregg Keizer  
September 25, 2010 05:10 PM ET [Comments \(20\)](#) [Recommended \(33\)](#) [f](#) [t](#) [Share](#)

---

Computerworld - Officials in Iran have confirmed that the Stuxnet worm infected at least 30,000 Windows PCs in the country, multiple Iranian news services reported on Saturday.

- Infected Siemens Programmable Logic Controller cards in nuclear power plants
- Suspected to be a targeted military attack against one Iranian nuclear plant
- Very sophisticated attack, using four 0-day exploits
- Infected thousands of Iranian systems
- Iran may have executed nuclear staff over this
  - Links Ch 9k – 9m

# SCADA Vulnerabilities and the Air Gap

Not in book

# SCADA Vulnerabilities

## 0-Day SCADA Exploits Released, Publicly Exposed Servers At Risk

**Italian researcher releases 0-day SCADA exploits leaving companies vulnerable to exploit; Emerging Threats project releases update to help detect attacks**

Sep 16, 2011 | 01:50 AM | [2 Comments](#)

By **John H. Sawyer**  
*Dark Reading*



Luigi Auriemma made news back in March 2011 with the release of 34 zero-day (0-day) SCADA vulnerabilities. This week, he's back in the news with the release of 15 new 0-day advisories, 13 of which affect eight different SCADA products.

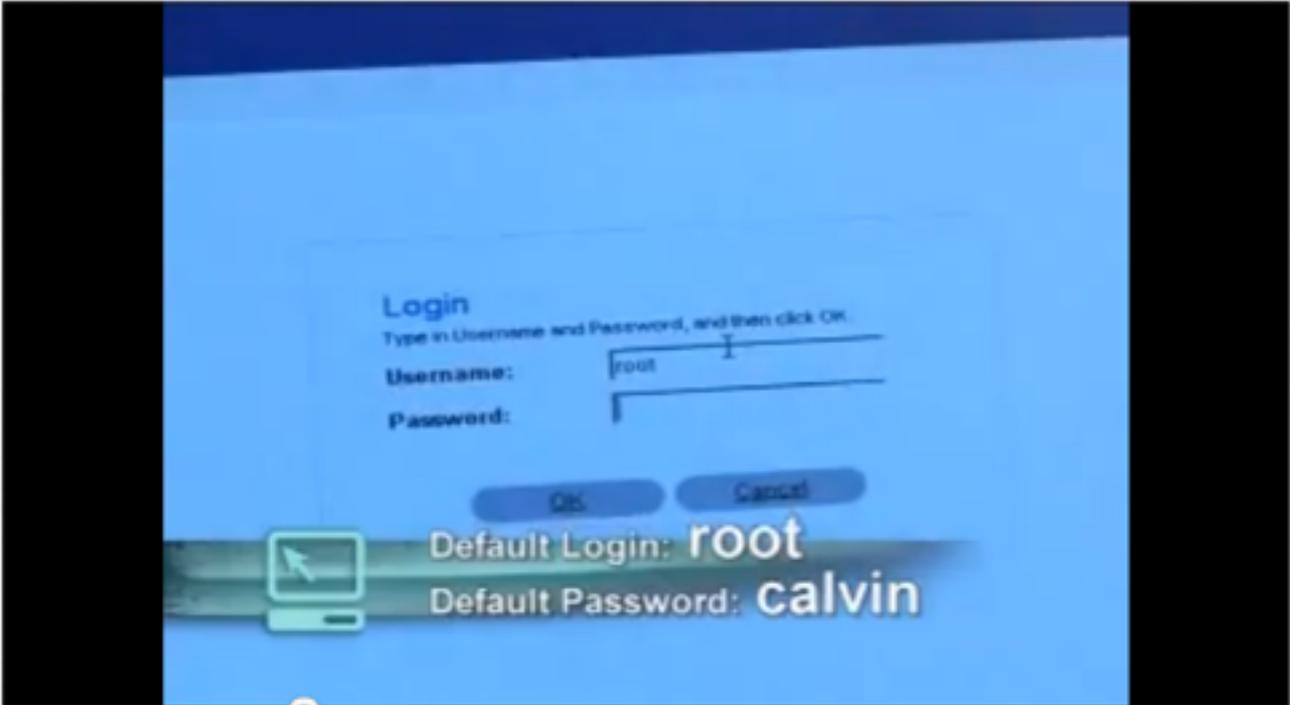
SCADA (supervisory control and data acquisition) systems monitor and control devices that can make physical changes in our world. Generally, they refer to systems that manage industrial, infrastructure, and facility processes – systems where vulnerabilities could have devastating impact.

\* [Link Ch 6b in CNIT 122](#)

# Dell DRAC Video

Remotely Administer a Server with DRAC

StudioDell + Subscribe 189 videos ▾



Default Login: **root**  
Default Password: **calvin**

2:07 / 9:23

\* [Link Ch 9q](#)

# 81 Vulnerable DRAC systems

\* Using SHODAN

\* Link Ch 9r

SHODAN "Remote Access Controller" port:80 Search

Results 1 - 10 of about 71 for "Remote

Top Countries	Count
United States	40
Belgium	10
Brazil	4
United Kingdom	4
Canada	3

Top Cities	Count
Laforêt	9
Charlotte	5
Atlanta	4
Scottsdale	3
São Paulo	3

Top Organizations	Count
Scottsdale Memorial He...	2
Carolina Internet	2
Boothel Internet	1
Affiliated Computer Se...	1

**Object moved**  
71.244.50.164  
Strange & Associates  
Added on 19.10.2012  
Lewisville

static-71-244-50-164.dlistx fios.verizon.net

HTTP/1.0 302 Object moved  
Date: Fri, 19 Oct 2012 08:46:41 GMT  
Server: Microsoft-IIS/6.0  
X-Powered-By: ASP.NET  
Location: http://remote.strangeepa.com/Citrix/AccessPlatform  
Content-Length: 171  
Content-Type: text/html  
Set-Cookie: ASPSESSIONIDQCTTQRAT=BCCJLIAECNIPLODNBE  
Cache-control: private

**Object moved**  
8.15.224.36  
ATI Solutions  
Added on 14.09.2012  
Molean

HTTP/1.0 302 Object moved  
Date: Fri, 14 Sep 2012 19:21:16 GMT  
Server: Microsoft-IIS/6.0  
X-Powered-By: ASP.NET  
Location: https://remote.oakviewbank.com/Citrix/AccessPlatform/  
Content-Length: 174  
Content-Type: text/html  
Set-Cookie: ASPSESSIONIDQAQATCSS=KCIHNBMBGFBMIBBFAHP

# Even Worse

## FACT CHECK: SCADA Systems Are Online Now

Saturday, September 24, 2011

Contributed By:  
Craig S Wright

Follow-Up Article: [SCADA: Air Gaps Do Not Exist](#)

\* \* \*



A recent "Fact Check" by [Scot Terban](#) requires some fact checking.

In his post, he basically shows that he has no idea how many SCADA systems are online. Scot stated "How about the fact that said systems are connected to the internet on a regular basis and SCADA aren't",

well this is a flaw and error of epic magnitude.

The fact is, nearly everything is connected now.

- \* **Later articles claim that many other systems are vulnerable, including passenger jets**
- \* **Links Ch 6d, 6e in CNIT 122**

# DHS Response

September 26, 2011, 3:30PM

## DHS Thinks Some SCADA Problems Are Too Big To Call "Bug"

by Paul Roberts

[Follow](#) @paulfroberts



10 Comments



The Stuxnet worm may be the most famous piece of malicious software ever written. When it was first detected, a little over a year ago, the worm sounded a warning to nations around the world that critical infrastructure systems were potential targets of attack for foreign governments and cyber criminal organizations alike. But with the anniversary of the Stuxnet worm's discovery just past, the Department of Homeland Security admits that it is now reevaluating whether it makes sense to warn the public about all of the security failings of industrial control system (ICS) and SCADA software.

\* **Link Ch 6f in CNIT 122**

# Cell Phones, Smartphones, and PDAs

- Conversations over traditional phones
  - Considered protected
    - Tapping used to require a lot of time, expensive equipment, and a warrant
  - Many have the same security expectations of cell phones, smartphones, and PDAs
    - PDAs have additional vulnerabilities associated with PDA applications and services
    - Smartphones combine functions; have even more vulnerabilities

# Cell Phones, Smartphones, and PDAs (cont'd.)

- Cell phone vulnerabilities
  - Attackers listening to your phone calls
  - Using the phone as a microphone
  - “Cloning” the phone to make long-distance calls
  - Get useful information for computer or network access
    - Steal trade or national security secrets
    - Java-based phone viruses

# Cell Phone Rootkit

## MALICIOUS SOFTWARE TURNS YOUR CELL PHONE AGAINST YOU

Smart phone malware could tap into your phone's microphone, GPS and even your battery.



By Eric Bland  
Tue Mar 9, 2010 07:00 AM ET  
4 Comments | [Leave a Comment](#)

Print

Email

Share

Tweet

digg

buzz



A rootkit is different – and more difficult to detect – than other malicious software like viruses.

iStockPhoto

### THE GIST:

- Phone malware could pose a bigger problem than computer viruses.
- Software can turn a cell phone's microphone, GPS and battery against the phone's owner.
- Cell phones may soon be an even bigger target for hackers than computers.

Malicious software for cell phones could pose a greater risk for consumer's personal and financial well-being than computer viruses, say scientists from Rutgers University.

The scientists have made a particularly resilient malware, known as a rootkit, that can turn a cell phone's microphone, GPS and battery against the phone's owner. The researchers say their work highlights the need for greater protection of cell phone software and greater awareness of cell phone vulnerabilities from owners.

- Link Ch 9I

# Rootkits

- Modify OS parts or install themselves as kernel modules, drivers, libraries, and applications
  - Exist for Windows and \*nix OSs
- Rootkit-detection tools and antivirus software
  - Detect rootkits and prevent installation
    - More difficult if OS has already been compromised
    - Rootkits can monitor OS for anti-rootkit tools and neutralize them
- Biggest threat
  - Infects firmware

# Rootkits (cont'd.)

- Trusted Platform Module (TPM)
  - Defense against low-level rootkits
    - Ensures OS hasn't been subverted or corrupted
    - ISO standard ISO/IEC 11889
    - Link Ch 9o
- Firmware rootkits
  - Hard to detect
    - Code for firmware often isn't checked for corruption
- Insider hacking
  - Harder to detect
    - Malicious code hidden in flash memory

# Rootkits (cont'd.)

- Systems compromised before purchased
  - May function like normal
  - Must flash (rewrite) BIOS, wipe hard drive, and reload OS
    - Expensive and time consuming
- LoJack for Laptops
  - Laptop theft-recovery service
  - Some design-level vulnerabilities rootkits can exploit
    - Infection residing in computer's BIOS
    - Call-home mechanism

# UEFI Secure Boot



The screenshot shows a web browser window with the address bar containing the URL: [blogs.msdn.com/b/b8/archive/2011/09/22/protecting-the-pre-os-environment-with-uefi.aspx](http://blogs.msdn.com/b/b8/archive/2011/09/22/protecting-the-pre-os-environment-with-uefi.aspx). The page title is "Building Windows 8" with the subtitle "An inside look from the Windows engineering team". The breadcrumb trail is "MSDN Blogs > Building Windows 8 > Protecting the pre-OS environment with UEFI". The main title of the article is "Protecting the pre-OS environment with UEFI". The author is Steven Sinofsky, dated 22 Sep 2011 3:00 PM, with 186 comments. There is a "RATE THIS" section with five stars, four of which are filled. The main text of the post is italicized and reads: "There have been some comments about how Microsoft implemented secure boot and unfortunately these seemed to synthesize scenarios that are not the case so we are going to use this post as a chance to further describe how UEFI enables secure boot and the options available to PC manufacturers. The most important thing to understand is that we are introducing capabilities that provide a no-compromise approach to security to customers that seek this out while at the same time full and complete control over the PC continues to be available. Tony Mangefeste on our Ecosystem team authored this post. --Steven".

- Link Ch 9o

# Best Practices for Protecting Embedded OSs

# Best Practices for Protecting Embedded OSs

- Include:
  - Identify all embedded systems in an organization
    - Prioritize systems or functions that depend on them
  - Follow least privileges principle for access
  - Use data transport encryption
  - Configure embedded systems securely
    - Use cryptographic measures
    - Install patches and updates
    - Restrict network access and reduce attack surface
    - Upgrade or replace systems that can't be fixed or pose unacceptable risks