Chapter 9 – Embedded Operating Systems: The Hidden Threat

Notes

Overview

This chapter provides an introduction to embedded operating systems. You will learn what embedded operating systems are, how to identify vulnerabilities, and practices used to protect them. These devices shouldn't be ignored simply because they're small, perform simple tasks, or haven't been exploited in the past. Security professionals should understand that any vulnerability in a desktop or server OS might exist for its embedded counterpart.

Chapter Objectives

After reading this chapter and completing the exercises, the student will be able to:

- Explain what embedded operating systems are and where they're used
- Describe Windows IoT (Internet of Things) and other embedded operating systems
- Identify vulnerabilities of embedded operating systems and best practices for protecting them

Tips

Introduction to Embedded Operating Systems

1. An embedded system is any computer system that isn't a general-purpose PC or server.

2. Embedded operating systems can be a small program developed specifically for use with embedded systems, or it can be a stripped-down version of an OS commonly used on general-purpose computers.

3. A real-time operating system (RTOS) is a type of specialized embedded OS typically used in devices such as programmable thermostats, appliance controls, and even spacecraft.

4. With just a cursory survey of a typical corporate building, you can find many embedded systems, including firewalls, switches, routers, Web-filtering appliances, etc.

5. Embedded systems are in all networks and perform essential functions, and that their security should not be dismissed.

6. As the value and quantity of targets with embedded systems increase, attackers will start shifting their focus to embedded systems.

Windows and Other Embedded Operating Systems

1. Software engineers recycle common code which has inherent risks.

2. Understand differences between Windows CE and Windows Embedded 8/Windows 10 IoT.

3. Unlike Windows CE, Windows 10 IoT provides the full Windows API and can perform many of the same tasks that the desktop version can.

4. You can run some vulnerability assessment tools on an embedded OS. There are also others that can be used remotely from the network to discover vulnerabilities in a Windows embedded OS.

Tip	Go to http://www.microsoft.com/windowsembedded/en-us/default.mspx for information on Windows embedded devices.

Other Proprietary Embedded OSs

1. VxWorks is an embedded OS widely used in many different environments and applications. It is designed to run efficiently on minimal hardware. A partial list of systems using VxWorks:
    a. Clementine spacecraft
    b. Deep Impact space probe
    c. James Webb Space Telescope (in development)
    d. Mars exploration rovers Spirit and Opportunity
    e. Mars Phoenix Lander
    f. Mars Reconnaissance Orbiter
    g. Radvision 3G communication equipment
    h. Stardust spacecraft
    i. SAUVIM (a submersible spacecraft designed for deep-ocean operations)

2. Green Hill Software also produces a variety of embedded OSs.

3. The multiple independent levels of security/safety (MILS) type of OS can run multiple levels of classification on the same CPU, without leakage between levels.

4. QNX is a commercial RTOS used by Cisco and Logitech.

5. Real-Time Executive for Multiprocessor Systems (RTEMS) is an open-source embedded OS used in space systems.

6. See Figure 9-2 for the difference between monolithic kernel and microkernel OSs.

*Nix Embedded OSs

1. Linux is an example of a monolithic OS used in a multitude of industrial, medical, and consumer items.

2. Embedded versions of Linux and other *nix OSs can be tailored for devices with limited memory or hard drive capacity.

3. Other versions of embedded Linux OSs (e.g., Real Time Linux and dd-wrt).

Tip	Visit http://nvd.nist.gov/nvd.cfm?cvename=CVE-2004-0075 for information on embedded operating system applications.

Vulnerabilities of Embedded OSs

1. Impacts of computer attacks are becoming more serious, including those targeted towards embedded systems.

2. The goal of many hackers today is to steal money.

Tip	Visit the following link for an article about eliminating embedded system software vulnerabilities: http://www.embedded.com/design/system-integration/4006645/A-proactive-strategy-for-eliminating-embedded-system-software-vulnerabilities-Part-2

Embedded OSs Are Everywhere

1. Today there are many more embedded devices that in 2000. They don't have the Y2K flaw, but they are under attack from hackers and terrorists who want to further their financial or political causes.

Embedded OSs Are Networked

1. Understand the advantages of connecting embedded devices to a network.

2. Questions that should be addressed for every machine or device on a network:
    a. What PCI devices are present?
    b. Where were they manufactured? Is the supply chain trustworthy?
    c. Which devices have embedded OSs stored in rewriteable (nonvolatile) memory?
    d. Which embedded OS is currently loaded on each device?
    e. Can you make sure the embedded OS hasn't been corrupted or subverted with malicious code?

Embedded OSs Are Difficult to Patch

1. Embedded devices are difficult to patch because they must continue operating regardless of threat.

2. Security testers must weigh the costs of fixing a vulnerable system against the importance of the information the embedded system controls.

Embedded OSs Are in Networking Devices

1. Networking devices, such as routers and switches, usually have software and hardware designed for the tasks of transmitting information across networks.

2. High-speed networks now use specialized hardware and embedded OSs.

3. When a hacker compromises a router they may have complete access to network resources.

Embedded OSs Are in Network Peripherals

1. The most common peripheral devices on an organization's network are printers, scanners, copiers, etc. Devices that perform more than one function are called multifunctional devices.

2. MFDs are attractive hacker targets because they are rarely scanned for vulnerabilities or configured for security.

3. See Figures 9-6 and 9-7 for how to set up custom links and modify firmware being uploaded on a Dell networked printer.

Tip	Visit http://cseweb.ucsd.edu/classes/fa01/cse221/projects/group2.pdf for a paper that presents a survey of several major embedded operating systems.

Supervisory Control and Data Acquisition Systems

1. Supervisory control and data acquisition (SCADA) systems are used for equipment monitoring in large industries and anywhere automation is critical.

Cell Phones, Smartphones, and PDAs

1. There additional vulnerabilities with cell phones, smartphones, and PDAs.

2. Trojan applications have become a big concern in mobile applications stores such as Google's Play Store and Apple's App Store.

Rootkits

1. Rootkits can modify parts of the OS or install themselves as kernel modules, drivers, libraries, and even applications.

2. Rootkit-detection tools and antivirus software can detect and prevent rootkits, but it is more difficult if the system is already compromised. Compromised devices may continue to function normally.

3. LoJack for Laptops, a popular laptop theft-recovery service, has some design-level vulnerabilities that rootkits can exploit.

Best Practices for Protecting Embedded OSs

1. Best practices for protecting embedded OSs:
    a. Identify all embedded systems in an organization.
    b. Prioritize the systems or functions that depend on these embedded systems.
    c. Follow the least privileges principle for access to embedded systems.
    d. Use data transport encryption, when possible, for embedded system communication.
    e. Configure embedded systems as securely as possible and follow manufacturers' recommendations.
    f. When possible, use cryptographic measures, such as TPM, for booting embedded systems, especially when a loss of data or a modification in the system's behavior is a major risk.
    g. Install patches and updates, when available, to address vulnerabilities. Make sure doing so is possible on the embedded system you're working with, however; some embedded systems can't have any downtime for installing updates and patches.
    h. Reduce the potential of vulnerabilities by restricting network access to only the IP addresses that need to communicate with embedded systems, and reduce the attack surface of embedded systems by disabling or blocking unneeded services.
    i. Upgrade or replace embedded systems that can't be fixed or pose an unacceptable risk.

Tip	Read about securing the Internet of Things at http://www.lynx.com/.

Additional Resources

1. Embedded Products OS/Software:
   http://components.arrow.com/embedded-computing/software/

2. Embedded Website:
   http://www.embedded.com/

3. OS Security and Information Assurance:
   http://www.lynuxworks.com/solutions/security.php

4. Windows 10 Internet of Things:
   https://www.microsoft.com/windowsembedded/en-us/windows-embedded.aspx

5. Embedded System Security:
   http://internetofthingsagenda.techtarget.com/definition/embedded-system-security

Key Terms

- **embedded operating system (OS)**
- **embedded system**
- **firmware**
- **multifunction devices (MFDs**
- **multiple independent levels of security/safety (MILS)**
- **real-time operating system (RTOS)**
- **supervisory control and data acquisition (SCADA) systems**