Treat your embedded systems equally

An embedded system contains a computing system that is dedicated to a specific function. When most people think about embedded systems in enterprise environments, they correctly identify devices such as routers, switches, and wireless access points. Even though people don't think of these devices as computers, they need to be managed as if they were — including securing them and keeping their software up to date.

The embedded systems most people don't think about include refrigerators, thermostats, door locks, handheld devices, smartphones, music players, and webcams. These devices represent the dark matter of the network universe; to the extent that they each have their own IP address, they represent as much or more of a security threat than the ones people think about. This means that you must treat these forgotten networked devices just as you would any other IT system: track them, secure them, maintain them, and manage their life cycle.

The rising threat

For years, embedded systems used purpose-built operating systems and software. The software had minimal functionality and limited access to the outside world, all of which minimized its vulnerability footprint.

In recent years, embedded system vendors have been using more general-purpose operating systems such as Linux and Microsoft Windows XP Embedded, shifting away from the traditional purpose-built systems such as Wind River VxWorks.

General-purpose operating systems can cost less to license, they can leverage open source software, and they can make software development cheaper and faster because software engineers already know how to program for Linux and Windows.

The result is that many embedded systems bring to your network the same operating systems and also the same vulnerabilities as desktop workstations and servers. These systems are flooding the workplace. Smartphones, hand-held medical devices, security systems, and environmental and process-control systems all have an IP address, and all represent a threat that must be managed.

One consequence is that a chorus of networked devices can amplify whatever worm or virus is able to infect your network. Think of your embedded systems relaying spam, participating in a distributed denial-of-service attack, hosting a worm that re-infects your internal systems, or acting as a port of entry to an intruder.

A targeted attack also can affect the very function of the embedded device, with consequences ranging from embarrassing to life threatening.

- Just google "unprotected webcams" and view images from around the world taken from webcams set with the default password, or no password. Embarrassing indeed, but consider the consequences of using the same vulnerability to turn off the webcam, open networked door locks, and walk right into your facility.
- An attack targeted at networked environmental control systems can raise the temperature in your server room and cause your servers to overheat and shut down. An attack against a city full of networked thermostats could have them all turn on the air conditioning at the same time and bring down the power grid.
- A denial-of-service attack against a networked medical device can cause it to spend so much time responding to network chatter that it gives false readings or fails to work at all, a situation that can result in injury or death.

Your action plan

With the risks posed by embedded systems more clear, the best way to manage them is by forming an action plan.

- Know what you have. Start by taking an inventory of your embedded devices. Hunt them down by making sure you know where every one of your IP addresses is used. Consult your DHCP server, and check your logs for signs of systems that are only on intermittently.
- Create an acceptance plan. Don't let just any device onto your network; set standards for what you will allow. Don't allow devices with fixed accounts or passwords. Give them the boot, or work with your vendor to get this issue fixed. Make sure that you have a plan for keeping the device's software up to date. Does the vendor supply updates? What is the cost? Can you apply Windows or Linux updates yourself?
- Bring existing devices up to snuff. Read the manuals and find default and maintenance accounts and make sure that they're not still set as the defaults. Find out what the devices' current software versions are, and update their firmware.
- Have a patching plan. Make sure you have a plan to track, and patch, vulnerabilities for all systems with an embedded operating system. If it connects to the network, chances are it needs to be regularly patched. Don't buy vendors' claims that embedded systems don't get viruses — that's just simply not true.

- Secure your networks. Put embedded devices onto separate firewalled networks as appropriate. For example, security devices including surveillance cameras, door locks, and environmental controls ought to be on a separate network with access only from your security system. Shared devices such as printers and multifunction copiers need their own DMZ network; most of your users need to talk to them, but they really shouldn't have a reason to initiate contact with other networks.
- Secure embedded devices. Use scanning tools to find out what unexpected and unnecessary services your embedded devices provide. Turn off the ones that aren't really needed. Can you telnet to your door lock? Probably not a good idea. Do you really need to be able to ftp to your printer? Only rarely. Can you turn services off as needed? If not, talk to your vendor. This is an area in which an inexpensive consumer device may cost more to manage than a more expensive, enterprise-quality device.
- Monitor, monitor, monitor. Monitor embedded devices with both an availability monitoring tool (such as Nagios) and your IDS platform. You should know the current state of every embedded system.
- Use life-cycle management. Track embedded devices as you would track any other IT asset. Manage their acquisition, deployment, maintenance, and disposal. Disposal is more than just proper recycling — consider the data that may be on a device before you dispose of it. Remember the disk drive in your copy machine.

The threat is real

The risk posed by embedded systems isn't just theoretical. The Stuxnet worm has been around for more than a year, and it has proved to be more virulent than expected, infecting PCs worldwide, and easily re-infecting systems on which it had been removed. As researchers have investigated the worm more thoroughly, they have discovered that it is the first one found in the wild that specifically targets and quietly disables process control systems that drive nuclear centrifuges. Its rapid spread may have helped it to penetrate the networks of its target organization. We may never learn the origin of this worm, but what we do know is that this is not the last worm we'll see.

Shine some light on the dark matter on your IP networks, and don't let hidden devices put your organization, employees, customers, or even the general public at risk. ■

A few embedded devices to worry about:

Checkout wands

Copiers

DVRs

Fixed medical devices (radiology systems)

Handheld medical devices (glucometer)

Inventory wands

Manufacturing control systems

Multifunction printer/copier/scanners

Network music players

Networked medical devices

Point of sale systems

Portable medical devices (echocardiograph, EKG machine)

Printers

Process control systems
- *Chemical plants*
- *Nuclear power plants*
- *Refineries*
- *Reservoirs*

Refrigerators

Scanners

Security cameras

Security sensors

Smart phones, iPhones, iPads, etc.

Televisions

Thermostats, environmental controls

Wireless access points

This article was reprinted from the Q3 2010 issue of The Barking Seal, a publication of AppliedTrust. You can subscribe to The Barking Seal online at http://www.appliedtrust.com/barkingseal.