Security

Best Practices for Industrial and Medical Devices

Six Strategies for Wind River VxWorks and Intel® vPro™ Technology

By Marc Brown, Vice President Tools & Marketing Operations, Wind River

Security is a top priority for industrial and medical devices, where system breaches can be life-threatening and economically devastating. Developers creating these systems need to consider security early in the product lifecycle and take a holistic approach to protecting their systems.

In this article we present a set of security best practices that form a foundation for good design. We also provide advice on how to implement these practices, citing practical applications of Wind River VxWorks, Wind River Hypervisor, and the future 3rd generation Intel® Core™ processor family.

The Growing Threat

Industrial systems are responsible for critical pieces of our infrastructure, such as water, electricity, oil, and natural gas. Cyber attacks could compromise the integrity of these essential systems, as well as cause significant economic damages and hardships. The Stuxnet worm, attributed to the 2010 infection of the Bushehr nuclear power plant in Iran, made international news, clearly demonstrating the risks to industrial systems. Indeed, security experts have counted an incredible 70 million unique instances of malware worldwide, making digital disruptions an ever-present threat.

Medical systems also make a tempting target. Responsible for maintaining or monitoring the health of patients, they frequently contain and exchange valuable patient information that could be used by criminals. Such breaches can be costly. According to the Second Annual Cost of Cyber Crime Study published in August 2011 by the Ponemon Institute, the median annual cost of cyber crime to an individual victim organization is $5.9 million per year. For devices responsible for patient care, an attack by a cyber threat could also severely impact human lives.

Despite the importance of these devices, many lack the strict security requirements or certifications seen in other fields like defense or government systems. Thus, it is often up to the developer to take a thoughtful approach to implementing security.

Best Practices for Security

In improving security, an excellent place to start is established industry best practices for secure computing. Below is a list of best practices considered integral to a comprehensive security strategy for connected devices. Some of these practices can be fulfilled by security solutions; others may require embedded customers to improve the way they administer and manage their devices.

- **Principle of least privilege** – Assign access privileges to an application, task or process involving devices and the network to be just enough to achieve the job at hand.
- **Depth in defense** – Include multiple layers of security to ensure if one layer is breached, others may still be able to protect the device.
- **Secure the weakest link** – Assume that the most vulnerable component, interface, or application is the most likely avenue of attack.
- **Failsafe stance** – Recognize that the best security plans come from those who expect the worse and act to carefully secure the network and all devices connected to it.
- **Secure by default** – Turn off any and all features, services, and access that are not necessary. If you’re not using it, don’t activate it.
- **Simple in design, simple to defend** – Select the simplest devices and usability designs that will do the job. They will be easier to configure, audit, and test.
Enabling a More Secure Configuration

To address three of these best practices—principle of least privilege, failsafe stance, and secure by default—start by recognizing that any system with connections to the outside world is subject to attack and will need a more secure configuration. This means restricting access privileges and enabling all security features. This last point is particularly important because security features are often unused by developers, leaving a system unnecessarily vulnerable.

To achieve a secure configuration, it’s important to follow manufacturer guidelines for enabling authorization and security features. These may include:

- Setting authorization and privilege levels to limit access to only authorized users.
- Giving authorized users the least privilege necessary for the services they’re expected to provide.
- Activating the network firewall.
- Disabling all non-essential services; enable only those essential to how your organization intends to use the device.
- Enabling or including robust cryptography libraries.
- Setting authorization (e.g. user names and passwords) as you would in a secure desktop or server environment. Deny “root” or highest privilege unless absolutely necessary.
- Enabling memory protection via the Memory Management Unit (MMU) to protect the kernel from user-mode applications running in real-time processes.

In setting up a medical or industrial device configuration, be sure to take advantage of any and all options provided by the real-time operating system (RTOS). A good example here is Wind River VxWorks®. In keeping with the best practice “simple in design, simple to defend,” most of its security features can be enabled through a single configuration option. This makes it easier to use its security features and helps ensure they’re activated.

Secure Network Communications

Many security issues in embedded systems stem from connections to networks that are open to a large population of users (e.g. an enterprise network) or directly to the Internet. For such systems, the network is clearly the weakest link. To maintain a failsafe stance, never assume that connectivity to and from a device is secure, or that a network is closed. Customers may connect your device in ways you did not anticipate.

To secure a device on a network, first enable the security features of the RTOS communications stack. For example, the VxWorks network stack that incorporates numerous security components such as a full-featured firewall that may be used out of the box (Figure 1).

To secure a device running VxWorks, a developer would:

- Enable the network firewall, opening only the essential TCP/IP and UDP/IP ports.
- Enable secure communication channels—e.g. IPsec, Security Sockets Layer (SSL) or Virtual Private Network (VPN).

Also look for RTOSs that are tested and certified by the Virtual Private Network Consortium for VPN compatibility. This certification provides extra assurance that an embedded device equipped with such an RTOS can easily participate with enterprise VPNs.

Developers should also carefully consider their hardware, and make sure the chosen platform has the performance to handle all of the security features. One such platform is the future 3rd generation Intel Core processor family, which will deliver multi-core performance, specialized Advanced Encryption Standard (AES) instructions, and a high-quality digital random number generator (DRNG). Together these features will enable high-performance packet processing, firewalls and other security features, and sophisticated application processing.

To illustrate the benefits of the platform, consider the processing requirements of IPsec and SSL. Both of these protocols can use AES encryption to create highly secure channels, but AES can impose significant processing overhead. The future 3rd Generation Intel Core processor family will address this concern with Intel® AES New Instructions (Intel® AES-NI), a set of seven instructions that significantly reduces encryption overhead. In addition, the new DRNG capabilities make encryption algorithms such as AES more secure by providing high-quality random numbers that potential adversaries cannot predict.

This processor family will also support Intel® vPro™ technology:

- Intel® Active Management Technology (Intel® AMT) provides remote management capabilities that can be used to recover compromised systems, even when they are powered off or in an unknown state.
- Intel® Trusted Execution Technology (Intel® TXT) provides malware protection at startup.
- Intel® Virtualization Technology (Intel® VT) improves the efficiency and security of virtualized environments.

![Figure 1. Wind River VxWorks includes a full-featured network stack.](image-url)
We will take a closer look at select features the future 3rd generation Intel Core processor family in the following sections.

Secure Data and Data Storage
As part of the depth of defense strategy, developers should consider data encryption, particularly for portable devices and devices with removable storage. In fact, data security is mandated by law for devices handling medical records. In the United States, these devices must conform to Federal Information Processing Standards (FIPS) or Health Insurance Portability and Accountability Act (HIPPA) regulations on patient data storage, which requires all communications, data, and storage used by the device to be secure.

As noted earlier, one potential drawback of data encryption is the processing overhead required. The Intel AES-NI instructions in future 3rd generation Intel Core processor family will significantly reduce this overhead, making techniques like full-disk encryption more attractive. In addition, the new DRNG capabilities will make this encryption more secure.

Partition to Protect Essential Components
Embedded systems today are leveraging multi-core platforms to combine a general purpose OS (GPOS), such as Linux* or Microsoft* Windows*, on the same platform with an embedded RTOS like VxWorks. This consolidation is made possible by a software layer known as a hypervisor that sits between the hardware and the OS. (Figure 2 illustrates one example: the Wind River Hypervisor.) The hypervisor abstracts the hardware and presents each OS with what appears to be a dedicated hardware platform.

The simple in design, simple to defend best practice would suggest the best security stance would be to keep a GPOS and RTOS apart. Thus, one key function of a hypervisor is to separate the guest OSs. This is a critical consideration from a security standpoint, because consolidation creates more potential entry points and can combine more-secure and less-secure software on one platform.

The security benefits of a partitioning OSs with a hypervisor are enhanced when deployed on the future 3rd generation Intel Core processor family. These processors include Intel® Virtualization Technology (Intel® VT) for IA-32, Intel® 64 and Intel® Architecture (Intel® VT-x) to help make virtualization more secure. Intel VT-x introduces hardware accelerators in the processor that trap and execute sensitive instructions. These accelerators relieve the hypervisor of these duties and significantly reduce the surface area exposed to attacks during handoffs between the standard OS and the RTOS.

This protection can be extended even further with Intel® Virtualization Technology (Intel® VT) for Directed I/O (Intel® VT-d). Intel VT-d securely assigns specific I/O devices to each OS to ensure that applications cannot receive one another’s data. This reduces resource competition and allows a mission-critical OS to continue operating even if another OS crashes. For example, if an OS running a human-machine interface (HMI) crashes, security-critical functions running in a different OS can continue to run.

Secure the Boot and Execution
Systems are especially vulnerable at boot time. Most full disk encryption schemes, for example, are vulnerable to a cold boot attack. Likewise, many systems (usually consumer-grade devices) can be maliciously re-flashed—i.e., reprogrammed in the firmware—to disable features or install malware. In these cases, how does one better secure the weakest link and provide depth in defense?

The answer is Intel TXT, another feature of the future 3rd generation Intel Core processor family. Intel TXT verifies the launch of a device at the firmware, hypervisor, and OS levels. Using an infrastructure known as the “root of trust,” Intel TXT checks consistency in behaviors and launch-time configurations against a verified benchmark called a “known good” sequence (see Figure 3). The system can then quickly
assess and alert against any attempts to alter or tamper with a system’s launch-time environment.

**Harden the System Against Attack**
Enabling security features alone doesn’t necessarily make a system secure. To address both the failsafe stance and the depth in defense best practices, security features must be designed, implemented, and tested for a variety of contingencies. For instance, to harden a system against a denial-of-service attacks or malformed data, a developer must increase the memory requirements for the network stack. This allows the stack to accommodate potentially huge data flows and maintain service.

To ensure their products work as advertised, developers should test security features such as user authorization, firewall, network protection, and other defenses. Unfortunately, this can be tough, time-consuming, or cost-prohibitive to personally do for a device. A good alternative is to look for certification of components by recognized organizations, like Wurldtech. Founded by a team of internationally recognized cyber security experts and industrial automation engineers, Wurldtech performs a brutal barrage of intrusion tests in certifying a product. VxWorks is an example of an RTOS that has achieved Wurldtech Achilles certification.

**Achieving Security Excellence**
Security is a journey, not a destination. No system is ever entirely secure or secure forever—new threats come into the world daily. Consequently, developing a secure system for industrial and medical systems involves taking a holistic approach based on the best practices for security provided in this article and a consideration of each device’s intended (and often unintended) environment and connections to the outside world. Taking advantage of the security features, technologies, and certifications available through VxWorks and the future 3rd generation Intel Core processor family will go a long way in improving the security of medical and industrial systems. It will also provide developers with an important competitive advantage in today’s fast-growing market for connected, intelligent devices.

Finally, keep in mind that embedded hardware and software companies and developers cannot do it all. Excellence in security requires an industry-wide effort. In particular, we must particularly make the effort to educate our end customers on the use of security technologies and application of these best practices in the real world in which they live.

For more on securing connected devices, see intel.com/go/embedded-security

---

**Contact Wind River**
Wind River Systems (intel.com/go/ea-windriver) is an Associate member of the Intel® Embedded Alliance. As a worldwide leader in embedded software and services, Wind River provides market-specific embedded platforms that integrate operating systems, development tools, and technologies.