WIND RIVER

Embedded Device Security in the New Connected Era

A true paradigm shift begins with a fresh perspective

By Marc Brown
Vice President for Tools and Marketing Operations

Executive Summary

Rapid growth in the intelligence and interconnectedness of embedded devices is accompanied by an upward spiral in security threats. Attacks on these devices are being perpetrated not only by the usual suspects but by a new breed of hackers supported by organized crime, nation states, and terrorist organizations.

Device developers must respond by taking a more holistic approach to device security—one that considers security issues at every layer of the development stack—from silicon to virtualization to the operating system, the network and communication stacks, and the application layer. This paper discusses the key considerations in delivering an end-to-end platform approach to device security and provides solid advice that can help you cut development time frames and costs, mitigate overall security risks, and transform security from a threat into an opportunity for competitive advantage.

Securing Embedded Devices

Many articles and papers about security try to scare the reader. What they should do instead is inform readers about the opportunity for innovation and competitive advantage. And nowhere is this opportunity more prevalent than in the world of embedded devices.

The recent surge in embedded device development has been remarkable. Around the globe, embedded products that control critical infrastructure are increasingly becoming intelligent, transforming from simple standalone to complex, autonomous connected control and monitoring. Today's embedded products are interacting not just with us—expanding our ability to communicate and share information—but with each other. They control smartphones; smart meters for our public utilities; industrial automation controls; transportation and oil and gas systems; communication networks; and mobile medical devices that literally keep people alive. Machine-to-machine interaction, delivered by ever smaller, ever smarter components, allows for new levels of sensor- and control-enabled analytics, revolutionizing business and government operations.

The sheer number and autonomy of these devices is also mushrooming. It is estimated that there will be more than 50 billion connected devices in use by 2020. Unfortunately, the rapid growth in embedded products is accompanied by an upward spiral in security threats. Each new device on the network is potentially the next weakest link. According to McAfee, more than 55,000 new malware programs and 200,000 zombies are uncovered every day, more than 2 million malicious websites exist, and new forms of attacks and exploits arrive daily. All these security threats are now accelerated by connected devices.

Equally alarming, security exploits are being perpetrated by a new breed of hackers. It's not just smart kids trying to breach a firewall for sport anymore. Increasingly, disgruntled current or former employees who have access to sensitive systems as well as knowledge of their internal workings are deliberately causing these systems to fail, using their insider's knowledge to execute sophisticated attacks. Professional, well-funded groups—including organized crime, government agencies, and terrorist cells—are finding security vulnerabilities through embedded devices and exploiting them in very creative ways. They're attempting to crack into secure networks, access sensitive information, and alter the behavior of safety critical systems, causing physical harm to equipment and potentially putting lives at risk. This is no longer the creative plot of the latest action and science fiction movie from Hollywood. It could be the foundation of future preemptive cyber-warfare.

Embedded devices have now become the targets of organized crime, nation states, and terrorist organizations.

Despite ever growing federal, state, local, and industry-specific security regulations and compliance requirements, cyber-attacks continue to succeed, as shown in these high-profile cases:

- Stuxnet, a sophisticated malware program, was unleashed against the Natanz nuclear enrichment site in Iran in mid-2009. Stuxnet was designed to infiltrate the control systems at Natanz and make hidden, damaging adjustments to vital centrifuges. The Stuxnet virus was also used against control system software in July of 2010, renewing long-standing concerns about whether the U.S. power grid can withstand targeted cyber-attacks. In this case, Stuxnet was designed to exploit a Windows zero-day flaw to find and steal industrial data from Supervisory Control and Data Acquisition (SCADA) systems.
- In 2008, a terminated employee of Hunter Watertech, in Australia, used a laptop with the firm's SCADA software and a Motorola two-way radio to issue wireless commands to the SCADA system of another firm, Maroochy Shire Council, that had decided not to hire him. He used the software to disable alarms in Maroochy Shire Council's sewage equipment and cause 800,000 liters of raw sewage to spill out into local parks and rivers.
- In 1997, perhaps the first documented successful attack on infrastructure occurred when a teenage hacker temporarily disabled a key telephone company computer servicing the Worcester, Massachusetts, airport, cutting off communication to the control tower and preventing access to emergency services (fire department, airport security, etc.).
- An infected laptop gave hackers access to computer systems

at a water treatment plant in Harrisburg, Pennsylvania, in October 2010. The laptop was used as an entry point to install a computer virus and spyware on the plant's computer system, according to a report by ABC News.

- In Poland, a teenage boy hacked into the tram system and derailed four vehicles—simply by adapting a television remote control so it could change track points. Twelve people were injured in one derailment, according to *The Telegraph*, a UK-based news publication.
- Cars seem to be the next hacking frontier. A terminated employee from a car dealership, the Texas Auto Center, logged into the company's web-based system and remotely set off horns in more than 100 vehicles on command and made it so drivers couldn't start their cars. The employee was later arrested on charges of computer intrusion.

In short, embedded devices have now become the targets of rogue employees, organized crime, nation states, and terrorist organizations looking to disrupt or destroy what was thought to be highly secure, well-protected infrastructure. And the costs of a security breach in these systems can be enormous. Major underpinnings of our economy and our infrastructure depend on embedded systems. A single successful attack can jeopardize everything from critical public services to the quality of health care. Ultimately, mission-critical activities and human lives are at stake in securing embedded devices.

Addressing Evolving Security Requirements

The key to preventing the new breed of security threats is to take a complete platform perspective rather than a piecemeal component approach to addressing security. Embedded device developers need to consider security issues at every layer—from hardware platforms and virtualization technologies to the operating system, the network stack, or other communications middleware, packets of data being sent across the network, and purpose-built applications required to support device functionality.

The first step is to conduct an end-to-end system security threat assessment that looks at security issues not just from the developer's viewpoint but from the perspective of manufacturers, operators, and end users.

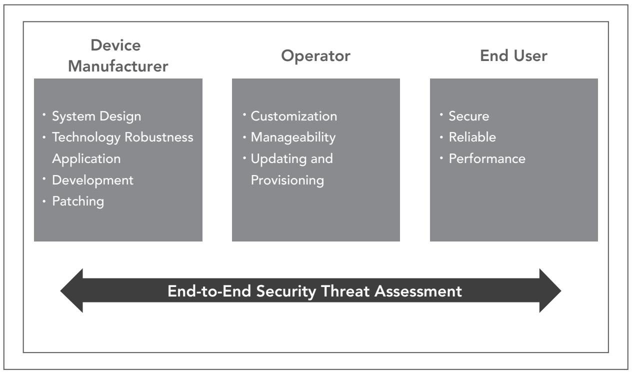

Figure 1: End-to-end security assessment

At the manufacturing level, for example, security needs to become an integral part of system design, specific technology selections, application development processes, and even application management tasks such as patching and upgrades. For operators, security threats inherent in configuration or customization must be analyzed and addressed. Software management, updating, and provisioning processes must also be designed with security in mind. At the end user level, the assessment should include security threats that can be introduced by the end-user, such as malware, viruses, worms, and trojans, all of which can affect reliability and performance.

> Embedded device developers need to consider security issues at every layer.

The security assessment must also look at potential vulnerabilities at each layer: virtualization, operating system, network stack, middleware, and application layer. At the virtualization or operating system layer, for example, developers need to be aware of how hackers seek to exploit an OS. Wind River's sensorpoint technology, delivered with Wind River Test Management, enables developers to easily simulate these techniques and ensure that a system behaves properly.

Once these vulnerabilities are understood, it becomes possible to use specific techniques to thwart attacks. For example, Wind River supports several higher-strength encryption keys and additional capabilities such as IPsec and Internet Key Exchange (IKE) and provides network stack compliance to FIPS 140-2 and testing against several security validation suites such as Common Criteria, Wurldtech, and so on. Wind River run-times are tested against the ever increasing techniques used to hack into an OS. In addition, Wind River provides security design guidelines to assist next-generation device development leveraging new techniques: separation via virtualization, certified run-time components, integration of "white-listing" technologies, and so on. Wind River also provides a comprehensive security-testing package with Wind River Test Management, enabling test teams to detect potential malicious code, simulate hacker attacks, and perform fuzz testing to ensure protocol robustness.

Securing the Software Stack

The next step is to drive security protection across the device system software stack—from silicon all the way to the application layer:

- **Silicon:** At the silicon level, there is an opportunity to embed technologies such as virtualization, trusted delivery, trusted boot, and others into the firmware of a chip to augment the robustness of the operating system.
- **Hypervisor:** Virtualization technologies can be used in unique ways to bolster security by the use of separation. Typically, many developers think about virtualization and its enterprise use cases of sharing system devices. However, to increase security in embedded devices, virtualization is being used more and more to separate device use, separate human machine interface (HMI) operating systems from the control operating system, separate the physical interface from the control operating system, and so on. This added use of separation within device designs can provide significant security improvements.
- **Operating system and communications stacks:** Operating system selection has become crucial for today's highly connected devices. The OS and communications stack should comply with the latest security requirements defined for the desired use. In addition, these products should be certified against market segment security validation suites; for example, industrial control device developers should look for OS/stacks validated against the Wurldtech Achilles certification. The Achilles program assesses the network robustness of devices and platforms and certifies that they pass a comprehensive set of security tests.

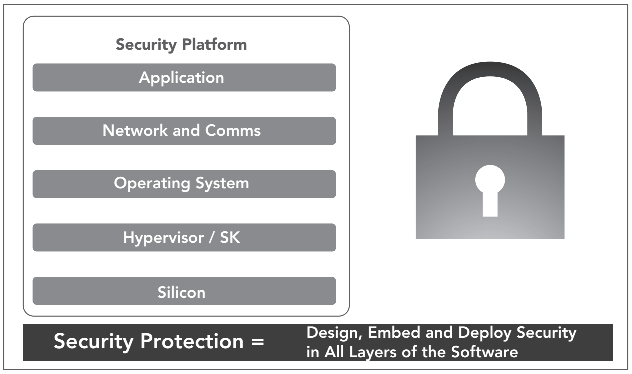

Figure 2: Security platform

- **Applications:** Applications need to be developed from the start with security in mind. Applications can take advantage of new technologies being developed to aid in security robustness, by leveraging "gray-listing" or white-listing. Developers need to design applications with strict security principles; otherwise, the device applications they deliver may be used as back doorways, ultimately for malicious use. The potential insertion of malicious code by rogue insiders or a network-based attack from the outside needs to be tested for and detected. Testing teams should be trained and equipped with the right set of tools to aid in security-focused testing and detection of unauthorized code modifications.

Increasing Importance of Certification

At every level, developers should be looking at ways to incorporate security design principles and associated security-certified run-time components: certified operating systems, certified network stacks, and certified middleware. Certification provides an independent validation from a trusted expert that a given component or platform meets specified standards and is conformant with specified requirements. It also provides a benchmark that can serve as a basis for comparison.

Dozens of equipment manufacturers have started to require certified assurances, given the increase in government regulations that are now being required in many markets and associated devices.

In the industrial automation arena, the Achilles certification program from Wurldtech is one of the most widely recognized. Embedded controllers, host devices, control applications, and network components can all achieve Achilles cyber-security certification.

Certification provides an independent validation from a trusted expert that a given component or platform meets specified standards.

When one looks more closely at the factors that are increasing cyber-vulnerability, the benefits of certification become even more pronounced:

- **Consolidation:** New technologies such as multi-core processors have created new cost-reduction opportunities for system consolidation. This in turn drives the need for industries to collaborate and set stronger standards and security paradigms for new devices that have combined previously separate functions. This is complicated further by new connectivity requirements. Cyber-security certification defines and validates conformance with these standards and paradigms.
- **Connectivity:** Everything from individual devices to factory floor systems is being connected to business systems, supply chain management systems, and the cloud. With the evolving machine-to-machine paradigm, and the connected "Internet of things," embedded devices have become exposed to unprecedented levels of vulnerability, leaving these embedded devices exposed to cyber-attacks. However, through cyber-security certification, standards can be established and risks can be controlled and mitigated.

Leveraging Application-Specific Technologies

Historically, security protection in the embedded space and in the application arena have been separate islands. However, given the increasingly connected nature of today's embedded devices, it has become a strategic imperative to deal with security threats holistically.

Since embedded devices have technology requirements that differ from traditional IT equipment—namely limited power, memory, and performance constraints—traditional security solutions are insufficient. With the teaming of McAfee and Wind River, embedded developers can implement security measures at all layers of the software stack, including the application layer.

Equally important, McAfee and Wind River can combine the concepts of white-listing and "reputation-based intelligence" to deliver stronger security to embedded devices. The white-listing approach, already commonplace in industrial, financial, medical, and enterprise data centers, focuses on allowing only the known good. By integrating these concepts with gray-listing, where security threat assessment is reputation-based, Wind River and McAfee can deliver a new security paradigm that addresses the full range of issues, threats, and exploits.

Using a Cyber-Security Certified RTOS

Wind River recently applied for and received cyber-security certification for its VxWorks real-time operating system. VxWorks was the first RTOS certified under the Achilles program. Wind River did this to enable its customers in the process automation, power and energy, oil and gas, transportation, and medical device markets to deploy an RTOS they could count on to mitigate the risks of cyber-attacks.

Specifically, VxWorks met the Achilles certification conformance requirements at Gigabit Ethernet, passing both 100Mbit and 1GigE certifications, which are recognized by most industrial and medical manufacturers to defend control devices against increased exposure to cyber-security attacks.

The Achilles program leverages Delphi, the world's largest database of industrial system vulnerabilities. It integrates specific vulnerability intelligence into common security enforcement devices such as firewalls and intrusion detection systems. This allows common IT infrastructure to be tailored for industrial network environments and continuously update specific rule sets and signatures, protecting control systems immediately and substantially reducing the frequency of patching activities.

As a result of this certification, developers can now leverage a pre-validated RTOS, which increases predictability, cuts development costs and time frames for building secure devices, and delivers something developers don't expect from an RTOS: peace of mind.

Wind River also complements the device-level cyber-security certification of VxWorks with data protection capabilities via the FIPS 140 standard, which enables customers to build their devices with hardened networking capabilities.

> Together McAfee and Wind River can combine the concepts of 'white-listing' and 'reputation-based intelligence' to deliver stronger security to embedded devices

Initial integration between Wind River Linux and McAfee security solutions will be followed by additional integration with other Wind River operating systems and embedded virtualization technologies. A phased rollout of security solutions will be delivered in 2011.

Conclusion

Clearly, it's time for a paradigm shift in embedded development. And in this case, a true paradigm shift begins with a fresh perspective about the importance of security—not just as a bolted-on feature, but as a built-in attribute of next-generation embedded devices. Simply put, developers need to design and architect embedded products to address security challenges before they become pervasive security problems.

By taking a platform perspective to security, and by harnessing the efficiencies of cyber-security-certified components, you can cut development costs and time frames while actually decreasing overall security risks. And that's more than a paradigm shift for embedded developers. It's a true transformation that delivers more secure infrastructure, stronger financial results, greater peace of mind, and a better way of life.

WIND RIVER

Wind River is a leader in embedded and mobile software. We enable companies to develop, run, and manage device software faster, better, at lower cost, and more reliably. www.windriver.com