WIND™
PROFESSIONAL SERVICES

PROFESSIONAL SERVICES SECURITY REVIEW FOR VXWORKS 7

Enabling Secure Deployment of Devices with VxWorks 7

Are you planning to use or are you currently building an embedded device using VxWorks® 7? Have you identified all of the security requirements for your device to protect your proprietary intellectual property and data against reverse engineering and theft? Are you relying on the myth of air gap security to protect your device against network-based attacks, or are you unsure how to implement secure communications with your device and protect it against evolving security threats? Work with the experts to ensure that security best practices are delivered in your project.

The VxWorks 7 SR0600 release now provides security capabilities that were previously only available to customers using the VxWorks Plus platform and Security Profile for VxWorks. These join a best-of-breed set of software-based security features that enable you to deliver cutting-edge, rock-solid security in your devices. This software solution includes:

- Secure Boot, which verifies during boot-up that binary images have not been tampered with or corrupted
- Secure Runtime Loader, which effectively protects the integrity of the system and safeguards your intellectual property from piracy and code from reverse engineering
- Full disk encryption, using AES, enabling secure data at rest
- Encrypted container support, using TrueCrypt-compatible AES-encrypted file containers, which safeguards data when the device is powered down
- Advanced user management, enabling protection from unauthorized access and enabling the definition and enforcement of user-based policies and permissions
- Enhanced network security through VxWorks 7 incorporation of the latest version of Wind River® SSL as well as Wind River SSH; Wind River cryptography libraries; and Wind River IPsec and IKE, the Wind River implementation of Internet Protocol Security and Internet Key Exchange, all to effectively secure network communications
- Time partitioning, to provide resilience against denial-of-service (DOS) network attacks
- Security events handler, which enables you to record and monitor conditions that could identify a potential security risk

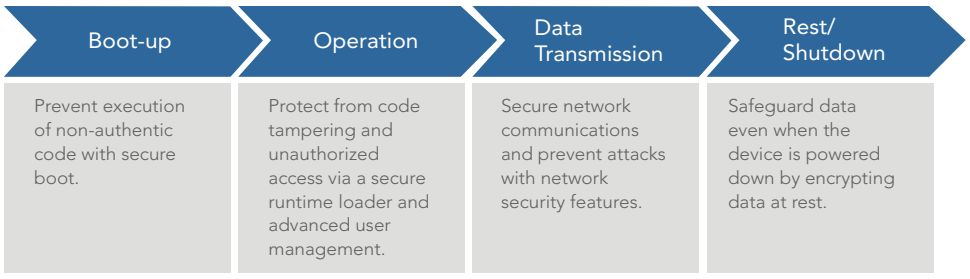

Figure 1. Protect connected devices at every stage with VxWorks

As a customer implementing VxWorks 7, you now have in your hands the tools required to build world-class, highly secure devices. However, as the never-ending data breaches in the industry make clear, simply having the tools is not enough. To build a secure system, you need security expertise. And no one knows more about securing Wind River VxWorks 7 than the cybersecurity experts from the Wind River Professional Services team.

The Wind River Professional Services team brings decades of experience in hardening embedded devices from cybersecurity threats. For a fixed price engagement, Wind River Professional Services will review your VxWorks 7 implementation and deliver a report that highlights:

- Possible security improvements by enabling AES, Secure Boot, Secure Runtime Loader, encrypted container support, and other features from the Security Profile.
- Review of your implementation of secure key storage and/or use of entropy sources. VxWorks 7 SR0610 release includes random number generation improvements, including optimized entropy collection, and passes NIST dieharder and TestU01.
- Review of your network encryption strategy: SSL configuration (TLS 1.2 with perfect forward security), usage of SSH, IPSec and/or IKE.
- Review of your VxWorks kernel configuration and compiler build options. From correcting simple mistakes such as leaving debug enabled to advanced recommendations to minimize the attack surface of your OS, no one is as knowledgeable about the myriad of available options as the Professional Services team from Wind River.
- Recommendations for minimization of side-channel attacks and other advanced threats.

DE-RISK THE SECURITY OF YOUR EMBEDDED DEVELOPMENT

Although valuable at any point in the product development lifecycle, the Wind River Professional Services Security Review for VxWorks 7 is a natural accompaniment to the initial development effort of a VxWorks 7 device. Security improvements are possible throughout the lifetime of an embedded device, but changes are much less costly in the initial design than when implemented after a device is deployed.

Wind River Professional Services can assist in:

- **The design phase:** Our report from the Security Review for VxWorks 7 can identify issues before a single line of code is written.
- **The implementation phase:** Review and optimize your VxWorks kernel configuration and compiler build settings before you start testing your application.
- **The testing phase:** Once your code is developed, our recommendations can direct improvements before the device is in the field.
- **Post-deployment use:** Even with devices in the field, our report may identify areas of improvement without platform changes. Some security enhancements can be provided by the deployment of organizational measures and corresponding controls.

For more information, please visit: www.windriver.com/services/#security.

WIND