WIND
AN INTEL COMPANY

SECURITY PROFILE FOR WIND RIVER LINUX

Open source software is increasingly being used across today's rapidly evolving devices and technologies. And as the footprint of embedded Linux expands, there is a need for stronger security capabilities. But the growing number of feature requirements, a highly innovative ecosystem, the increasing demand for availability, and the compliance required to address common vulnerabilities pose an exponentially increasing challenge to developers.

Leveraging deep experience in embedded Linux, Security Profile for Wind River® Linux provides vital security capabilities on top of open source innovation to cover a broad spectrum of silicon architectures and vertical markets.

Security Profile is a commercial off-the-shelf (COTS) product designed to enhance the security posture of deployed systems and the data that resides on them. The hardened kernel, enhanced user space, and Yocto Project 2.0 compatible base seamlessly integrate with validation tools, documentation, and hardware support. Security Profile helps customers shorten their development lifecycle and achieve faster time-to-market with the improved security, performance, user experience, and manageability required for today's devices.

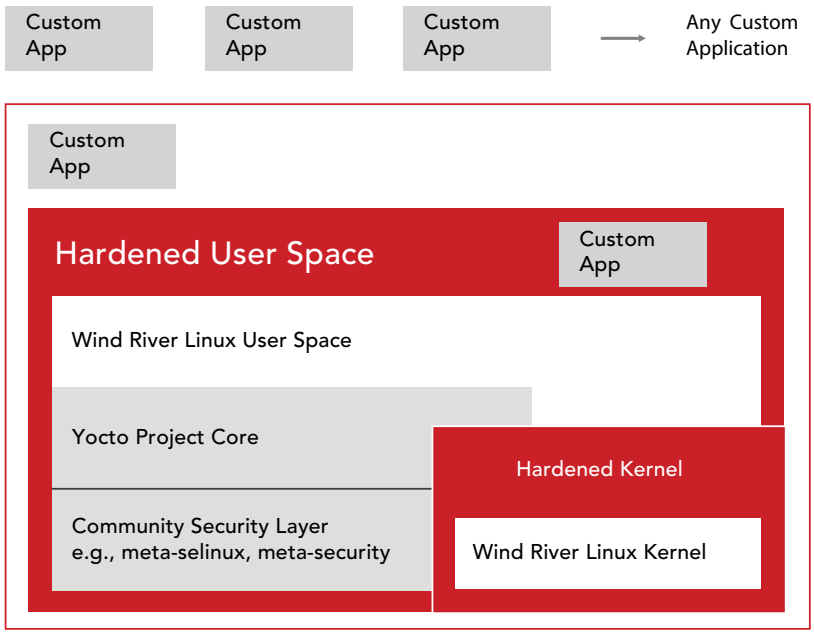

Figure 1: Security Profile for Wind River Linux architecture overview

KEY BENEFITS

The security requirements common to sectors with regulatory constraints—such as aerospace and defense—have migrated in recent years to other industries, as more devices become connected and require increased security. Now, the networking, industrial, automotive, and Internet of Things (IoT) sectors are facing the same challenges. Because we need to trust data to make decisions, especially in IoT, security is critical—which means the data must be secured along all parts of the its path, from device to cloud. Multiple levels of protection are needed: for the systems of trust and control, the device itself, the applications, and the data (both at rest and in flight).

Referring to the same set of security standards can ensure connected software products are consistent, but this presents a challenge for developers creating secure products using embedded Linux. Meeting these requirements can be expensive and time consuming, adding cost and risk to any program. Wind River helps manufacturers reduce these risks with the following:

- **Long-term security monitoring:** Wind River monitors new security risks and provides timely fixes, with a remediation process that allows customers to keep the security features of their products up to date.
- **Cost reduction:** Wind River reduces the cost of developing and maintaining a full-featured Linux distribution with security enhancements that align with those used by many industries and standards organizations.
- **Risk reduction:** With Security Profile, your product will remain compliant with applicable security standards.
- **Accelerated time-to-market:** COTS software reduces development time and allows you to focus on value-added features.
- **On-device protection:** Features such as mandatory access control, our full user space memory protection feature, and the ability to easily remove known weak encryption algorithms from the system insulate customers from security flaws.
- **Detailed system monitoring and forensics:** Intrusion detection and prevention tools give system owners configurable levels of monitoring, including real-time notification of security-relevant events. Extensive auditing tools provide valuable insights into the nature of any compromise if one occurs.

KEY FEATURES

Security threats against Linux-based devices are becoming more common as the number of connected devices increases. Threats include unauthorized access, data and device destruction, information disclosure, modification of information, and denial of service. Security Profile provides the features necessary to fight these threats, following the three well-known information security components of confidentiality, integrity, and availability (known as the CIA triad). These are the foundational security principles for the protection of an asset.

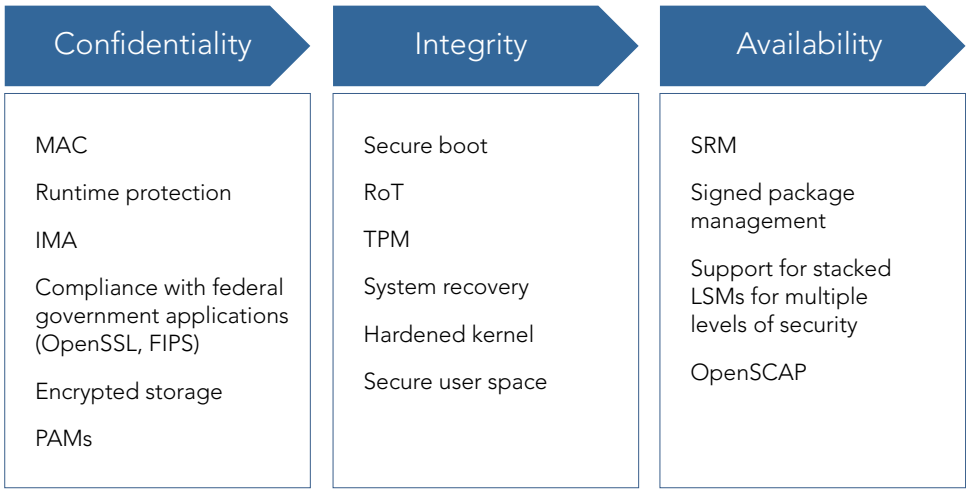

Figure 2. Security Profile features related to the three foundational security principles

Security Profile features fall under the three CIA components as follows:

Confidentiality

- **Access control:** Security Profile includes identification and authentication, discretionary access control (DAC), cryptographic, and audit services. It provides required security services and assurances for processing administrative, private, sensitive, or proprietary information. In addition, it enables the containment of untrusted programs through its type enforcement feature and user accounts configuration. Its rich and flexible security policy is scalable to include a broad application ecosystem.
- **Runtime protection:** Security Profile provides multiple implementations of mandatory access controls (MACs). This well-regarded technology in the security community has achieved significant adoption, as well as a suite of integrated features that bring a complete set of security improvements and ease of use with its configuration-free operation. Its comprehensive memory protection includes both compile-time and runtime stack protection against buffer overflows and address-space randomization. Security Profile also provides a complete hardened solution with access control lists ((ACLs) as well as file system and network protection.
- **Software integrity:** Integrity managed architecture (IMA) and secure remote management (SRM) are tests that verify the application has not been tampered with before allowing the device to load and run software.
- **Pluggable authentication modules (PAMs):** These packages add authentication, authorization, and auditing support to your secure platform.

Integrity

- **Secure boot:** Security for the boot process helps ensure that system firmware running on the device is the desired firmware and has not been replaced or tampered with.
- **Root of trust (RoT):** A base for trusted computing ensures the software running on the system hasn't been tampered with.

- **System recovery:** When a system is compromised, the included recovery and manageability tools can provide clean up of the system, prevent attacks from happening again, track which system resources were compromised, and identify those portions no longer trustworthy.
- **Trusted platform management (TPM):** Security features used for generating keys, securely storing passwords, certificates, or encryption keys, and storing platform-specific measurements ensure the integrity of the platform.
- **Hardened kernel:** The new unified secure kernel enables kernel hardening features with the new WRSECURITY configuration option. The secure kernel features enhanced address space layout randomization (ASLR), memory sanitization, and prevention of certain memory corruption-based exploits.
- **Secure user space:** Secure-core and secure-platform options—built to take full advantage of run-time buffer overflow protection and including a suite of tools aimed at locking down, monitoring, and auditing a system—give administrators more insight and more control of the system than ever before.

Availability

- **OpenSSL and FIPS:** Security Profile includes support for OpenSSL with FIPS for compliance with federal government applications.
- **dm-crypt partitioning, firewall, and encrypted storage:** Encrypted storage ensures that the data you maintain will be specific to the device and cannot be modified on another device or system.
- **Package management:** Packages must be maintained to ensure they are up to date with the latest security enhancements and defect fixes, as well as with any functionality enhancements.
- **Yocto Project Compatible:** This open source solution is based on the Wind River Linux Yocto Project 2.0 Compatible platform.
- **Linux Security Modules (LSMs):** Support for stacked LSMs allows multiple levels of security.
- **Compliance to standards:** Security Profile complies with Internet Protocol Security (IPsec), security associations (SAs), and other standards.
- **OpenSCAP**: This tool helps configure deployed systems in a secure manner and maintain the secure configuration.

CONTACT US

To learn more about the Wind River Linux product line, visit www.windriver.com/products/linux.
To have a representative contact you, call +1-800-545-9463 or write to inquiries@windriver.com.

WIND
AN INTEL COMPANY

Wind River is a global leader in delivering software for the Internet of Things. The company's technology is found in more than 2 billion devices, backed by world-class professional services and customer support. Wind River delivers the software and expertise that enable the innovation and deployment of safe, secure, and reliable intelligent systems.