Kevlar Embedded Security

Go above and beyond meeting requirements for your Linux-based embedded system

Cyber Resiliency   Vulnerability Reduction   Flexible Configuration

LAYERED LINUX CYBERSECURITY FOR EMBEDDED SYSTEMS

Designed using a threat model that assumes an attacker will gain administrative access to the system, Star Lab's **Kevlar Embedded Security** maintains the integrity and confidentiality of critical applications, data, and configurations at rest, through system boot, at runtime, and during updates in the field.

1. **Compatibility** with Intel x86_64 platforms and ARM64 platforms allows Kevlar Embedded Security to secure Linux-based embedded devices across industries. Integrated with Yocto and WindRiver LTS21 and LTS22 Linux.

2. **Flexible Security** Kevlar Embedded Security is a flexible, layered security solution providing defense in depth to your Linux-based embedded device. You choose the security layers, Kevlar Embedded Security does the rest.

3. **Cyber Resilience** Kevlar Embedded Security doesn't keep malicious actors out. It protects the system, even if malicious actors have already broken in. Prevent an attacker from changing your sensitive applications and data, even with root.

4. **Balance Your Performance** Kevlar Embedded Security lets you choose how much (or how little) security you layer into your embedded system. Secure what you need, where you need it, so you don't have to compromise performance.

5. **Testable Security** Kevlar Embedded Security comes with a full test suite, allowing you to verify the security bits are working as expected and generating the artifacts necessary for certification and accreditation.

Kevlar Embedded Security goes beyond helping you meet NIST, IEC, and SAE cybersecurity requirement by building cyber resilient systems through basic cyber hygiene, integrated (and centralized) logging and auditing capabilities, and enabling immutable systems that, once deployed, cannot change.

Reduce Cybersecurity Risks on Linux Embedded Systems

1 Prevents offline modification and replacement of binaries

2 Preserves application functionality through attacks

3 Prevent introduction of malware after deployment

4 Builds security "walls" around apps and services

5 Enables existing kernel hardening protections

6 Only allows signed kernel modules on system

7 Limits reloading the kernel or kernel-like applications

8 Disables various memory interfaces

8 Removes direct access to peripherals

10 Enforces lockdown mode independently of secure boot

11 Forces application to use explicitly defined sys. calls

12 Prevents and mitigates some classes of CVEs

LEARN MORE

Kevlar Embedded Security

Flexible Cybersecurity Layers for Linux-based Embedded Devices

Example Use Case

The Challenge

An industrial manufacturer producing ruggedized tablets running Wind River® Linux is concerned that their tablets could easily fall into the hands of a malicious actor, either because a tablet gets stolen, misplaced, or surreptitiously purchased. If a malicious actor were to get a tablet, they could discover ways to uniquely identify devices online, look for weaknesses in communication protocols, tamper with the physical device and extract the firmware / software, analyze the extracted code for vulnerabilities, and / or determine ways to load malicious code. Given these tablets are used in industrial manufacturing, any compromise in the system and any resulting disruption or damage could destroy the company's trustworthiness or have second- and third-order effects throughout the industrial industry.

In the past, the team was satisfied with very basic security, such as device passcodes, but now a single tablet can enable someone to control much of the infrastructure as well as influence the data used by decision-making algorithms running on backend systems. The team sees now how important securing the tablets is for its customers. They need to act.

The Solution

Star Lab's Kevlar Embedded Security can deny a malicious actor the ability to perform many of the standard tamper and reverse engineering activities necessary to pinpoint vulnerabilities and craft specific exploit payloads that impact operations. This is important if a device is to be introduced into a hostile environment where the threat of in-place physical tamper is present, but it also reduces the threat to commercially available devices where anyone can acquire a device and perform vulnerability research.

The Result

Most malicious actors are lazy; they target the easiest of targets. If a device is even slightly difficult to obtain, analyze, or exploit, malicious actors will move on to simpler, less time-consuming targets. Using Kevlar Embedded Security from Star Lab pulls a device out of this low-hanging-fruit category, making it an easy way to radically increase a device's security.

KEVLAR
EMBEDDED SECURITY

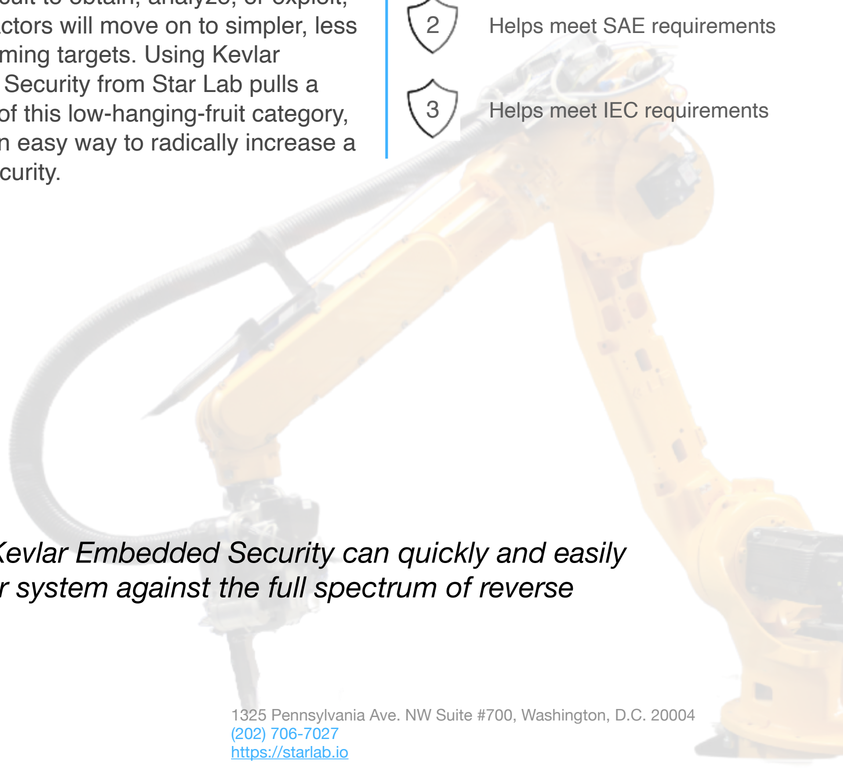
Meeting Certified Security Requirements

Kevlar Embedded Security helps you meet your internal and/or external cybersecurity requirements with ease:

1 Helps meet NIST requirements

2 Helps meet SAE requirements

3 Helps meet IEC requirements



Contact us if you are interested in learning how Kevlar Embedded Security can quickly and easily meet your security requirements and protect your system against the full spectrum of reverse engineering and cyber-attacks.

STAR LAB
A WIND RIVER COMPANY
SOFTWARE

1325 Pennsylvania Ave. NW Suite #700, Washington, D.C. 20004
(202) 706-7027
https://starlab.io