PROVE & RUN

www.provenrun.com

PROVENCORE-M for ARMv8-M

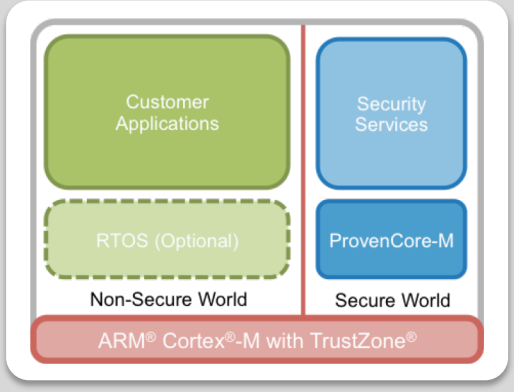
ProvenCore-M for ARMv8-M is a new version of ProvenCore-M, Prove & Run's next-generation of ultra-secure RTOS, providing a Trusted Execution Environment (TEE) running in the ARM® TrustZone root of trust in ARMv8-M processors such as ARM Cortex®-M23 and Cortex-M33.

ProvenCore-M is designed to help secure embedded devices based on microcontrollers such as gateways, IoT sensors and actuators, communication devices, etc. ProvenCore-M enables devices makers and solution developers to rely on an off-the-shelf, scalable and certifiable secured-by-design platform for their IoT devices that integrates easily into existing and new architectures.

The ARMv8-M version of ProvenCore-M allows extended versatility and provides certified security features for sensitive security services running on top of it such as secure boot, firmware update, secure storage, etc..

Why Use ProvenCore-M

Embedded devices are increasingly facing cybersecurity issues originating from the lack of robustness of their software stacks, with hackers exploiting bugs and weaknesses. On one hand, devices are more connected than ever, through a variety of communication links: deeply embedded devices are now just one hack away from the Internet. On the other hand, they are required to carry increasingly sensitive industrial operations, involving cyber-physical systems or dealing with confidential and/or personal data, performing sensitive transactions, creating or forwarding valuable data while safekeeping their authenticity, etc. At the same time, time-to-market and cost pressures are unyielding, and designers need to reuse existing code and drivers, and even whole RTOSs (FreeRTOS, AUTOSAR, etc.) that have not been designed with security in mind and cannot be trusted as such.



ProvenCore-M addresses these challenges head-on: it provides a set of security services to customer applications that covers all common needs. In effect ProvenCore-M and its security services can be use to deploy a "security perimeter" around a device that brings a high level of protection to customer applications.

ProvenCore-M is built using formal methods to be as close as possible to "zero-bugs" and therefore highly resistant to attacks. Using formal methods also makes ProvenCore-M and its security services much easier to certify.

Furthermore, thanks to the TrustZone feature of the ARMv8-M architecture, ProvenCore-M for ARMv8-M runs transparently alongside the customer applications, even if the customer applications require a RTOS. Therefore ProvenCore-M for ARMv8-M integrates easily into new and existing devices. By bringing strong security foundations, ProvenCore-M simplifies the design, implementation, maintenance and certification of scalable secure embedded systems.

Security Services

The security services supported by ProvenCore-M can be easily invoked using entry point functions call from the Non-Secure World. A few examples of potential security services:

- Secure Boot: Validating the authenticity of all software components.
- Over-the-Air Firmware Update: Remotely updating the firmware.
- TLS Client: Forcing applications running on the Non-Secure World to communicate with remote servers only through a secure authenticated channel.
- Secure Storage: Protecting the authenticity and confidentiality of sensitive data (e.g. secret keys).
- Cryptographic Services: Processing sensitive cryptographic computation in a protected environment, with dedicated countermeasures to improve resilience to attacks.

77 avenue Niel, 75017 Paris, France - +33 1 75 77 55 55 - contact@provenrun.com