CodeMeter Security and VxWorks 7

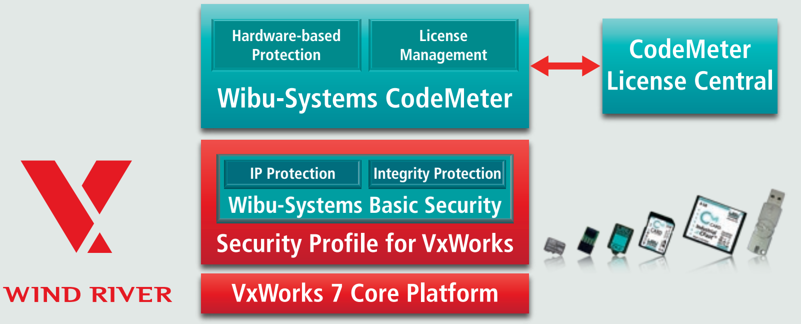
Powering more than 1.5 billion embedded devices, VxWorks is the world's most popular real-time operating system. The users of VxWorks are increasingly interested in security measures that are quick and simple to integrate. CodeMeter technology is compatible with the VxWorks development environment and the operating system itself. With VxWorks 7, using modern security protection technology is even easier.

The constant stream of news about security exploits and industrial espionage is powering a new demand for embedded systems that are designed to be inherently secure without relying on external protection systems like firewalls or VPNs. Mechanical engineers would call such devices intrinsically secure. Devices without significant security capabilities will find fewer and fewer buyers in the foreseeable future. At the same time, the developers of applications that run on embedded systems want to protect their intellectual property (IP). The security solutions should allow maximum protection with minimum effort. After all, not every user is also an expert cryptographer. The needs of both target groups – the developers and plant engineers, and the users and operators – were considered in the design of the new Security Profile for VxWorks 7.

To make it easier for end users to work with cryptographically protected software and secure boot procedures, Wind River has teamed up with Wibu-Systems to include Wibu-Systems' technology in Security Profile for VxWorks. The profile is being sold by Wind River and can be used as a plug-in for developers' workbenches. In addition to Wind River-developed features, it includes tried and tested components from Wibu-Systems that have been part of VxWorks since version 6.8. The operating system image, the kernel modules, and the applications are still encrypted by ExProtector. ExProtector and the CodeMeter Embedded driver (now as Version 1.7) are both part of Security Profile package.

The difference is that Security Profile works without CodeMeter Dongles or computer-specific licenses. The protection is purely software-based, but embedded deep in the VxWorks kernel. The solution therefore complies with two essential security requirements: integrity and know-how protection. The integrity of the individual software components is protected by cryptographic signatures. The VxWorks development environment includes its own certification authority (CA) that produces, signs, and manages the required certificates. The software vendor can provide a certificate for every developer involved in the project, which identifies the developer and determines his or her permissions. Even in large-scale projects, this makes sure that only named developers have the right to modify kernel modules or generate new VxWorks images. Every developer signs off his or her work with a personal certificate. When the finished software is run on an embedded system, the Secure ELF (Executable and Linkable Format) loader checks the chain of certificates immediately in the operating system to establish whether the signatures are valid. If this is not the case, the application will not run.

For our non-IT specialist readers: If a single bit or parameter is changed – for whatever reason – in a signed application, the signature is automatically voided. Checking the signature makes sure that the application has not been tampered with and that it comes from an authorized developer who alone has the right key.



Signatures protect applications from tampering and make sure they are from an authorized source. In order to avoid the theft of intellectual property by means of reverse engineering, software developers also need to encrypt their code. This is also possible with Security Profile: when setting up a new VxWorks project, an AES key is created for encrypting all modules and applications. The files protected in this manner are distributed in encrypted form only, while the right keys are kept at both the software vendor's and on the embedded systems. The Secure ELF loader decrypts the files in the operating system only when an application is launched. The necessary function is integrated in VxWorks itself and needs no adjustments on the part of the developers.

Secure Boot

Developers or plant engineers want to make sure that their machines controls only use software they have tested and approved and that the controls cannot be tampered with. This level of protection is already possible for the software itself in the form of code signatures. Making sure that the operating system, i.e. VxWorks, itself has not been manipulated needs a secure boot function, which was previously discussed in KEYnote issue 26. Platforms that support UEFI (the successor to the former BIOS) can make sure that only approved and signed software is run from the very first booting to the launching of individual applications. A key function of UEFI is its support for secure booting: the bootloader itself is checked, which launches only signed firmware images to run signed applications only. UEFI is the secure anchor that holds the entire secure boot chain in place.

CodeMeter Security

Security Profile is fully compatible with CodeMeter Security. Keys can be stored in hardware dongles (CmDongles) or system-specific soft licenses (CmActLicenses). In addition to the secure storage of the keys, CodeMeter also adds copy protection, as neither a CmDongle nor a CmActLicense can be copied.

In addition, CodeMeter Security allows the use of flexible licensing models and works with CodeMeter License Central to create and issue licenses. This paves the way for novel business models for embedded devices, such as the leasing of production equipment, pay-per-use concepts, or the secure monitoring of allowed production runs and batch sizes. CodeMeter Security also helps emulate the success of the after-sales business in the overall consumer industry and in the smartphone industry, which is experiencing particularly rapid growth.

Devices can be delivered with all features ready for use, but the client is limited to the features that his or her license covers. All other features remain off-limits until the right license has been bought. This saves considerable effort for product development, testing, and certification.

Security Profile offers a comfortable entry point for embedded security with cryptographic technology based on AES and elliptic curves. Secure Boot makes sure that applications can be run in a trusted environment.

CodeMeter Security is the option of choice for users wanting to add flexible license management, copy protection, and high security standards to their keystores. CodeMeter Security is based on established mechanisms and is distributed by Wibu-Systems as an add-on for development environments.

Complementarity of Security Profile and CodeMeter Security

Integrity	✓
Authenticity	✓
IP Protection	✓
Certificates	✓
Copy Protection	optional CodeMeter Security
License Management	optional CodeMeter Security
Hardware Key Storage Containers	optional CodeMeter Security