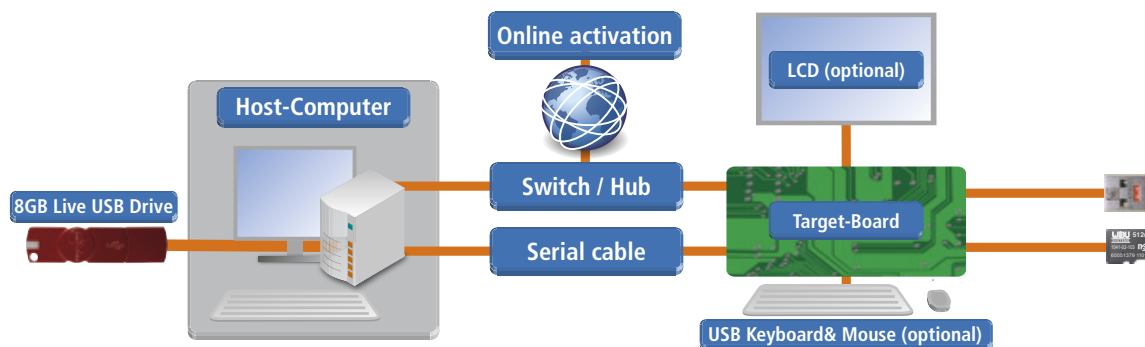# VxWorks EDK with WindRiver

The Embedded Development Kit for VxWorks is the result of a collaboration between Wind River, Emerson and Wibu-Systems. The EDK allows developers to protect their know-how and products from piracy, reverse engineering and attacks. It prevents code from being manipulated, and ensures the operating system and the developers' applications are securely booted and executed. Flexible pricing models such as pay per use or feature on demand facilitate the implementation of new business models.

The AxProtector plugin for Eclipse protects several different types of projects, e.g. VxWorks images (VIP), downloadable kernel modules (DKM) and real time processes (RTP). All configuration settings are made in the Wind River Workbench and include settings for reverse engineering protection, license management, signatures to protect the code from manipulation, parameters for license management and code encryption, and a key source for the private key which is used to sign the code.

CodeMeter has been modified for VxWorks to allow integration into the Eclipse-based Wind River Workbench. Developers can now protect their code without the need to use external tools.

The step-by-step instructions and illustrative examples explain usage in a wide range of areas:

- Encryption of program code for protection from software piracy
- Reverse engineering protection of profit-making know-how in algorithms
- Integrity protection to prevent program code being tampered with, e.g. in cyber attacks
- Feature on demand as a business enabler for new business models

The scope of delivery of the Wind River EDK includes an Emerson NITX-315 board with an Intel Atom processor and three CmDongles. The VxWorks development environment is started directly from the CmStick/M which is connected to the host computer. The CmCard/µSD with the VxWorks boot image and the required CodeMeter licenses is inserted into the target board. The CmStick/C is connected to the target board. This dongle contains a license to enable other software features in the image, as and when required.

To use the security and license management functions, the standard VxWorks loader must be replaced by the CodeMeter VxWorks loader. This ensures only correctly signed projects can be executed and decrypted on the target system.

Signatures and certificates

When the protected VxWorks project starts on the target system, its integrity is verified by CodeMeter. AxProtector generates the signatures in a three stage process using asymmetric cryptography with elliptic curves (ECDSA, Elliptic Curve Digital Signature Algorithm):

1. AxProtector signs the checksum, or more precisely, the hash value of the project or program code with the private key. The signed hash value is referred to as the signature and is a digital fingerprint of the project.
2. The modified VxWorks loader also calculates the hash value and compares it with the digital signature. The public key is required here to check the two hash values are the same and hence verify the fingerprint.
3. If verification is successful the VxWorks project is considered unchanged and not tampered with since it was signed with the genuine private key.

WIBU SYSTEMS

Certificates are needed to make sure a genuine public key is used for verification. Certificates are the digital equivalent of identity documents in real life. They check whether the stored public key really belongs to the corresponding private key.

Certificate chain

Wibu-Systems uses a series of certificates, known as a "chain of trust", to verify the authenticity of the public key. A certificate is verified through the use of another certificate, hence creating a chain of certificates which ends with the root certificate, the so-called "anchor of trust." Trust is thus passed to the level above. The key value is stored in the respective public key. A detailed description of the certificate chain is given below:
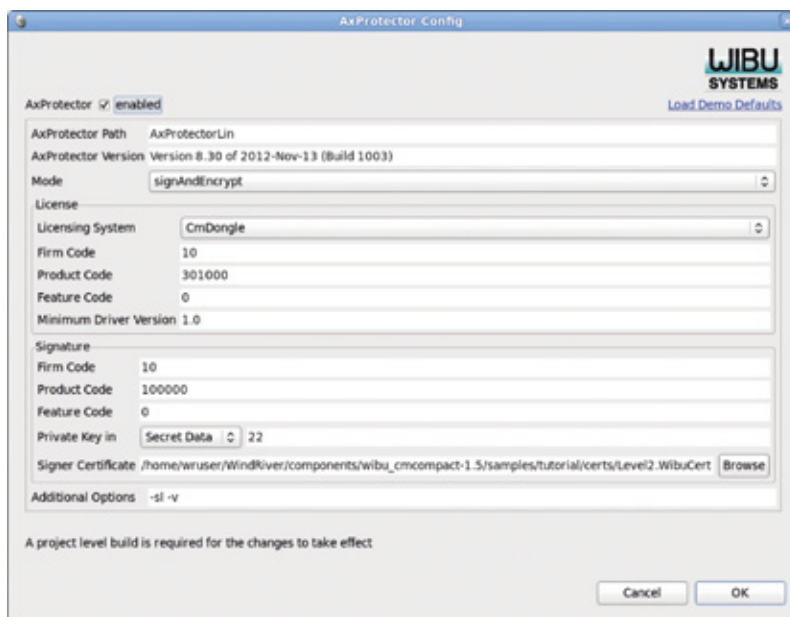
1. The developer uses the AxProtector configuration settings to define and create an integrity certificate containing a hash value, the signature and the public key.
2. As soon as the VxWorks project has been loaded, the VxWorks loader calculates the binary hash value and compares it with the hash value generated by AxProtector in the integrity certificate. If the values differ, the VxWorks project is not loaded.
3. If the hash values are the same, signature verification via the certificates begins. Each level of signature verification uses the public key of the level below until the root certificate is reached.

Although at first glance this process appears to be very complicated, its integration into the system has been carried out in such a way as to make it easy for developers to use. Its major benefit is that it requires the most important secret, i.e. the private key of the root certificate, to be used only once to sign the lower level certificates. Afterward it can be returned to its safe. If a certificate ever becomes compromised, a "revocation mechanism", which will not be explained here, can be called to revoke the certificate. In this way the security and integrity of the overall system is maintained and rolled out systems need never be superseded.

License generation, management and rollout

Alongside the security functions, it is also important to integrate the generation and distribution of licenses and keys into the sales and production processes. CodeMeter License Central is the right solution for this. The software is operated via a browser or web interface and can be easily incorporated into existing ERP systems such as SAP or MS Dynamics, CRM systems such as Sales Force, or online shops. License Central can be operated by the vendor or used in a Wibu-Cloud solution.

The Wind River EDK demonstrates to developers how the different functions can be protected in different ways in an application. Accordingly each function requires its own license before it can be executed in the live application. This can be beneficial if the aim is to sell device functions on an individual basis, for example, as part of an after sales service. It also allows activation of specific functions for particular groups of people such as service technicians.

All configuration settings for Wibu-Systems AxProtector are made via a plugin in the Wind River Workbench

WIBU SYSTEMS