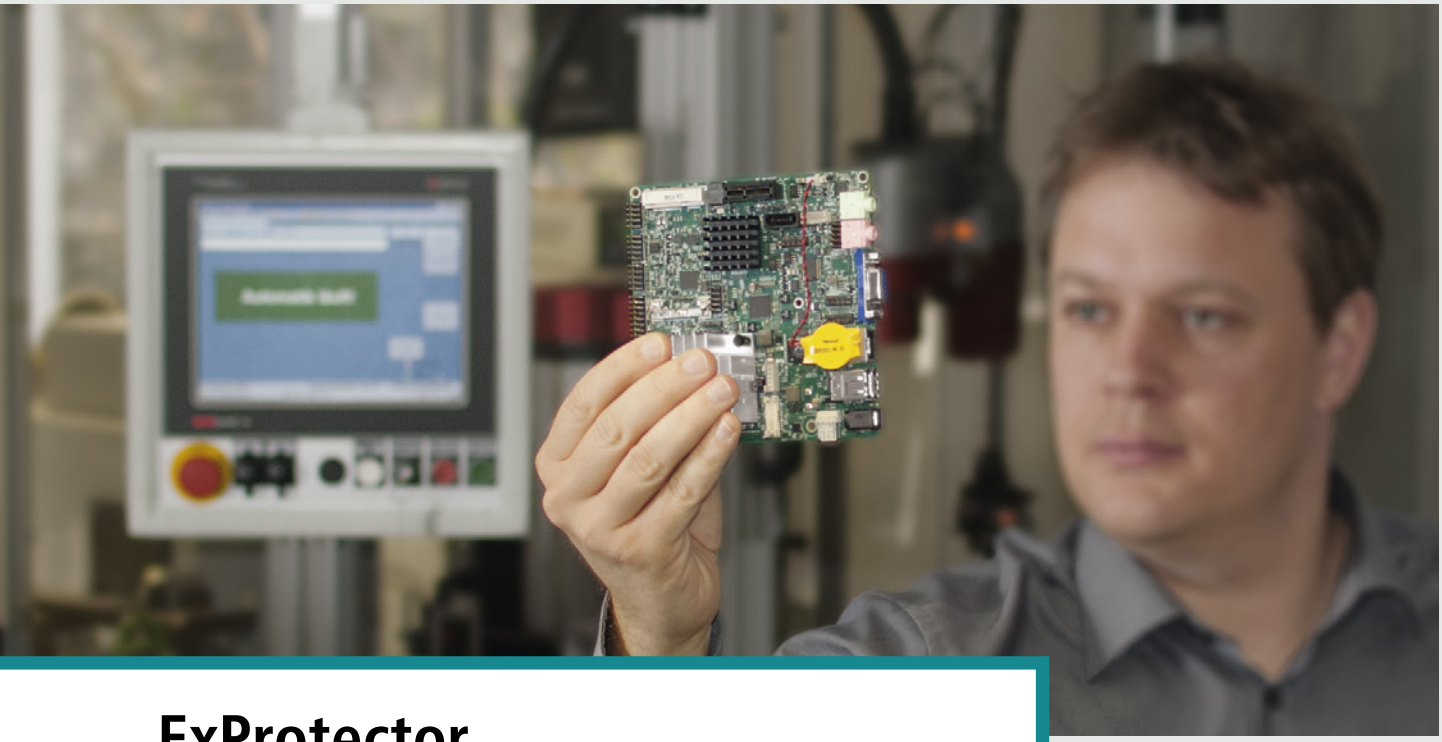


ExProtector

The world is changing. Smaller, connected computers are used more and more around us. They are pushing out the old proprietary solutions in all technical aspects of industry and even in our everyday lives. Wibu-Systems offers manufacturers and users simple-to-use tools to protect their systems and know-how.

The market for embedded systems continues to grow. Controllers that used to rely on specific and dedicated functions are being replaced with powerful and versatile computers, independent systems with the familiar traits that we all know from desktop PCs. Besides CPU and RAM, they come with flash memory storage, sometimes displays, network ports, and typically a number of USB ports. These systems tend to operate with specialized versions of common desktop operating systems like Linux, Windows Embedded, or VxWorks, with the newest kid on the block being Android, which has become a favorite for many small-scale systems. The routers that most people use for internet access are one type of such embedded systems, but smartphones and tablet computers can also be considered embedded devices. On a larger scale, modern cars come with a multitude of similar systems. In the manufacturing industry, machines work with PLCs. Building controls, CCTV cameras, automatic doors, traffic lights, smart meters, and even airliner avionics rely on embedded systems. In essence, all these disparate technologies use a similar architecture.

The devices need to be programmed, maintained, and increasingly supervised, and controlled from the outside. The interfaces used for that purpose employ common standards: Local access relies on USB or Bluetooth; in networks, the systems can be reached by their IP address, using Ethernet, WLAN, or industrial field busses.

With all of these components increasingly interconnected with each other and with standard operating systems used for versatile and powerful platforms, new avenues are also open for attack and intrusion that the former proprietary systems without network or USB access did not offer potential perpetrators.

Targets

Attacks usually have one of two purposes: the theft or the manipulation of software and data. The victims can be the producers of the system or machine, or their users. The reasons behind these attacks can be attributed to one of four categories:

A Theft of the know-how of the plant manufacturer (control software, type of implementation, possible exploits)

B Theft of the know-how of the plant operator (formulas, process parameters, log files)

C Manipulation of the operating data by the system operator to hide any improper usage, make illicit warranty claims, or tamper with the records for pay-by-use models.

D Sabotage by disgruntled workers, competitors, or secret services. The highest-profile historical incident in this respect is the Stuxnet attack.

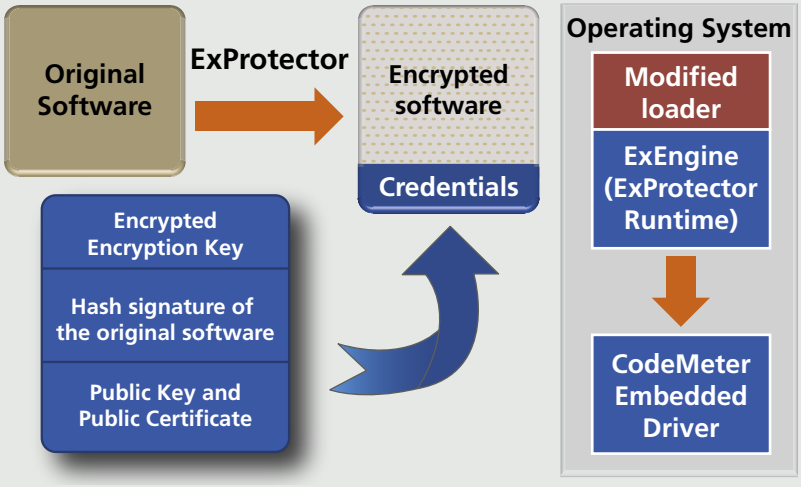
Wibu-Systems' Protection Suite for PCs and Embedded Systems

The increasingly loud call for better protection for industrial applications and data has encouraged Wibu-Systems in its commitment to improving protection in the sector with its Protection Suite. In traditional PCs, memory or processing power are not an issue anymore, whereas embedded systems often use small-scale, resource-efficient architectures. Open systems like VxWorks, Android, or Linux also play a more prominent role here than they do in the desktop world, as they allow individual adjustments to the given needs.

AxProtector, for PCs, and ExProtector, for embedded devices, are able to encrypt complete applications or single libraries securely without any change to the applications source code. The CodeMeter software takes care of decrypting these files for the run-time environment and scans for any potential attacks.

AxProtector creates an encrypted archive of the original application code and adds self-extraction functionality as well as the necessary license parameters to authorize the decryption by the CodeMeter runtime. This adds only a few kilobytes to the encrypted file. After the archive has been authorized and extracted, it checks its integrity automatically.

Embedded systems often have higher requirements in terms of real-time capabilities, while having less memory and processing power than their desktop counterparts. That's why we optimized AxProtector concept for embedded systems' specific restrictions.



Process of integrity check

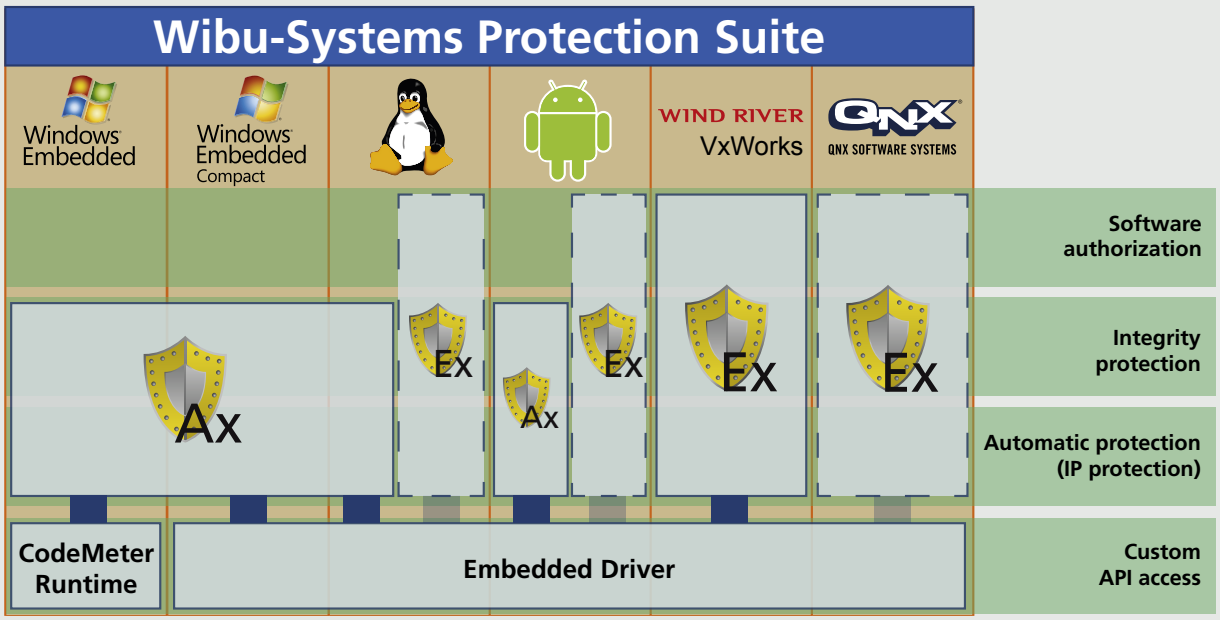
ExProtector

ExProtector encrypts applications, libraries, or data files for embedded systems. The encrypted file includes only a handful of additional bytes with the license parameters required for decryption and the signed hash (checksum) in the header.

All cryptographic functionality is already built into the operating system itself, including the drivers for accessing licenses on dongles or software-based CmActLicenses as native code.

Wind River offers VxWorks with the CodeMeter Loader completely integrated from the start. A similar integration in Linux and Android is easy because of the flexible modifications allowed by these operating systems.

This deep integration in the operating system makes for greater efficiency and greater security. The Loader uses the hashes and signatures to check the integrity of the applications or files encrypted by ExProtector after their authorization and extraction. Combined with secure boot procedures, which CodeMeter's technology also covers, one can produce a completely copy- and tamper-proof system without the need for additional software.



Wibu-Systems Protection Suite with the current Protectors (solid border) and planned Protectors (striped border)