Security Partner

WIBU SYSTEMS

Partner Use Case

Endpoint security to safeguard railway control systems

Real-time capable intellectual property and integrity protection for power converter systems in railways

Product

SLE 97

Security Partner

Use case

Application context and security requirement

A leading manufacturer of electrical systems for railways wanted to protect their know-how invested in their software against counterfeiting, reverse engineering, and tampering. Wibu developed a technology - CodeMeter® Embedded - protecting the integrity of the machine code.

Challenge

The vendor manufactures a real-time controller for the electric power system of trains. The unit is therefore used in harsh conditions with public safety implications. Even though it employs failsafes, a power outage can cause inconvenience for passengers, and could lead to delays across the entire network, and cause other safety concerns. The challenge is not just building a robust controlling software for the power converter system, but also making sure it stays secure from local and remote cyber-attacks.

Implementation

The vendor had two major requirements: the security of the controller system in a scenario exposed to wide temperature and moisture variations, and the protection of its IP and liability. Within six months, a security system was developed and integrated into the controller system. To prevent the software from being analyzed or pirated, the firmware was encrypted in the secure environment of the vendor, before being first downloaded at the contractor's production facilities.

Operating the system was made secure with an industrial-grade dongle with the form factor of a SD card that is used on every embedded system. The device provides a trust anchor during the secure boot and decrypts the controller software just in time. This is done only in its designated hardware environment and in association with a valid license. All cryptographic processes run at startup or under separate threads without impacting on the real-time operation of the controller system.

User benefits

› Know-how protection achieved by encrypting the controller software
› Integrity protection obtained with a secure boot process and the use of CodeMeter dongles as secure elements
› Real-time capabilities preserved by using cryptography during the startup phase or in separate threads

Security Partner

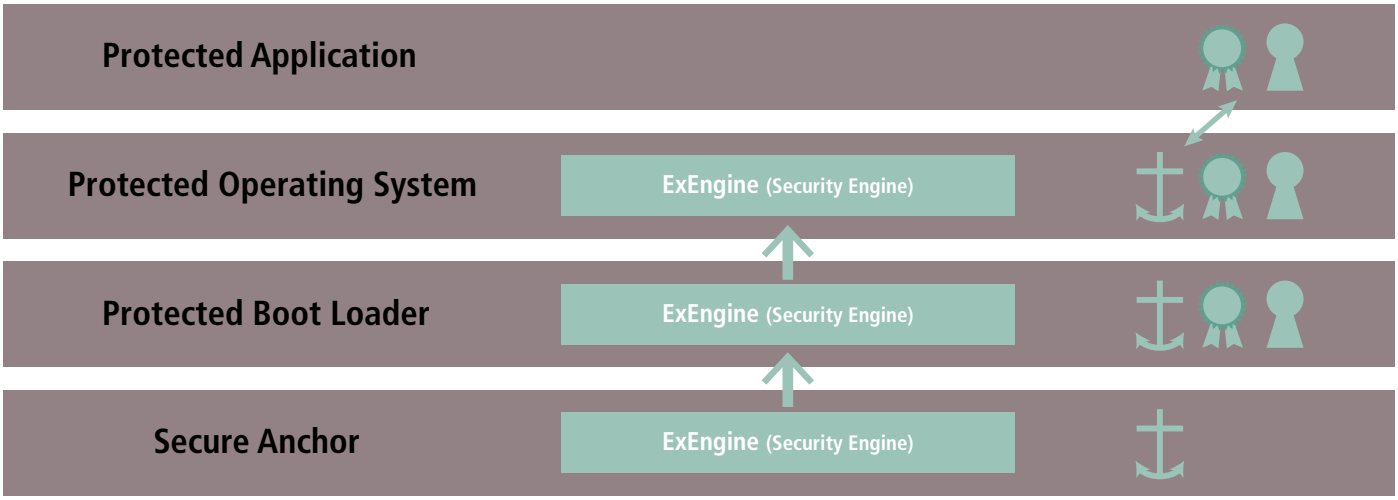
Solution

In the delineation of the project the safety relevance of the application was paramount. Hardware components had to comply with an extended operating temperature range, moisture challenges, and vibrational conditions. The software security elements were to guarantee high security to cyberthreats, and be compatible with the real-time operating system already in use. The multiplicity of attack vectors on the territory called for an endpoint security solution, and the replicability of the model was to allow repetitive sales internationally. CodeMeter met all these criteria and was then integrated into the existing power controlling infrastructure.

After developing and testing the controller software at the manufacturer's site, the file is directly encrypted. The cryptographic keys are stored in a USB dongle that embeds a smartcard chip. The foreign contractor manufacturing the power converter loads the encrypted file into the controller and plugs a SD Card into the system. A license is generated online with the dongle of the manufacturer and preloaded on the card. This gives the manufacturer control over the volume of devices produced, and ensures that the contractor cannot get in touch with the decryption keys.

The operating system of the controller is based on VxWorks. After powering up the system, the bootloader decrypts the VxWorks image, loads it and checks its integrity. The main application is then decrypted, loaded and checked. All necessary keys are stored in the secure memory of the dongle. The cryptographic operations occur inside the smartcard chip so that the keys never leave the secure area. CodeMeter's technology is therefore integrated both with VxWorks and the target system in order to support a secure boot process and a complete workflow from the bootloader to the application.

All cryptographic processes make use of industry standards like Advanced Encryption Standard and elliptic curve cryptography. Both algorithms are supported natively by the smartcard controller.



Main benefits of the Infineon product

The SLE 97 microcontrollers provide all the necessary cryptographic algorithms and security certifications for state-of-the-art security chips, as well as the computing power and memory capacity for a fast and future proof dongle. Additionally, this family fulfills the extended temperature requirements (-25°C to 85°C to soon be upgraded to -40°C to 105°C) typical of industrial applications.

Partner

Partners from the Infineon Security Partner Network help you secure your devices and applications: understand which threats can undermine your business, propose solutions that will protect your business, build and implement such security solutions and, when relevant manage their operation. They have been selected by Infineon on the basis of their system security competence and ability to design and deliver strong and trustworthy security solutions. Their activities are diverse and include security consulting, security solution provision, electronic design, systems integration and trust services management. For some, offers are off-the-shelf, while for others, offers are custom-built.

Wibu-Systems
Wibu-Systems is an innovative technology leader in the global software license entitlement market.

In its mission to deliver unique, most secure and highly flexible technologies to software publishers and intelligent device manufacturers, Wibu-Systems has developed a suite of hardware- and software-based solutions dedicated to the integrity protection of digital assets and intellectual property. Its product portfolio addresses a wide variety of license delivery models, including personal computers, Programmable Logic Controllers, mobile, embedded systems, cloud computing, software as a service, and virtualized architectures.

Through its motto “Perfection in Protection, Licensing and Security”, Wibu-Systems reinforces its commitment to eradicate software counterfeiting, reverse-engineering, code tampering, as well as device and smart factory sabotage, espionage and cyber-attacks.

Headquartered in Karlsruhe, Germany, Wibu-Systems holds subsidiaries in USA and China; the company also has sales offices in Belgium, France, the Netherlands, Portugal, Spain, the United Kingdom, and a capillary world distribution network.

Wibu-System’s contribution to the Infineon Security Partner Network
More than the sum of its parts: Infineon’s and Wibu-Systems’ complementary technologies have broadened the range of applications for both companies.

Over its history, Wibu-Systems has broadened its focus to embrace not just Independent Software Vendors, but also industrial automation. With a vocation to provide intelligent device manufacturers with industrial-grade units, Wibu-Systems has powered its entire hardware product line with the SLE 97 security controller made by Infineon Technologies, an ARM® SecurCore® SC300TM, 32-bit, USB 2.0 full speed, CC EAL 5+ certified crucial component for the data security and system integrity of computers and embedded systems in smart factories.

Additionally, Wibu-Systems has successfully integrated the embedded variant of CodeMeter® (its flagship solution for software protection, licensing, and security) with Infineon’s XMC4000 industrial microcontroller family. Software developers of field programmable gate arrays and microcontrollers can now protect application code and intellectual property against reverse engineering and implement a license control system.

Published by
Infineon Technologies AG
81726 Munich, Germany

Date: 05 / 2016

Additional information
For further information on technologies, our products, the application of our products, delivery terms and conditions and/or prices please contact your nearest Infineon Technologies office (www.infineon.com).

Please note!
THIS DOCUMENT IS FOR INFORMATION PURPOSES ONLY AND ANY INFORMATION GIVEN HEREIN SHALL IN NO EVENT BE REGARDED AS A WARRANTY, GUARANTEE OR DESCRIPTION OF ANY FUNCTIONALITY, CONDITIONS AND/OR QUALITY OF OUR PRODUCTS OR ANY SUITABILITY FOR A PARTICULAR PURPOSE. WITH REGARD TO THE TECHNICAL SPECIFICATIONS OF OUR PRODUCTS, WE KINDLY ASK YOU TO REFER TO THE RELEVANT PRODUCT DATA SHEETS PROVIDED BY US. OUR CUSTOMERS AND THEIR TECHNICAL DEPARTMENTS ARE REQUIRED TO EVALUATE THE SUITABILITY OF OUR PRODUCTS FOR THE INTENDED APPLICATION.

WE RESERVE THE RIGHT TO CHANGE THIS DOCUMENT AND/OR THE INFORMATION GIVEN HEREIN AT ANY TIME.

Warnings
Due to technical requirements, our products may contain dangerous substances. For information on the types in question please contact your nearest Infineon Technologies office.

Except as otherwise explicitly approved by us in a written document signed by authorized representatives of Infineon Technologies, our products may not be used in any life endangering applications, including but not limited to medical, nuclear, military, life critical or any other applications where a failure of the product or any consequences of the use thereof can result in personal injury.