CASE STUDY: INDUSTRIAL INTERNET IN ACTION

Endpoint Security to Safeguard Railway Control Systems

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

EXECUTIVE SUMMARY

A leading manufacturer of electrical systems for railways wanted to protect their know-how invested in their software against counterfeiting, reverse engineering, and tampering. Utilizing Infineon's SLE 97 security controller, Wibu-Systems developed a technology - CodeMeter® Embedded - protecting the integrity of the machine code.

THE 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 fail-safes, 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.

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.

THE 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 cyber threats, 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 with the target system in order to support a secure boot process and a complete workflow from the bootloader to the application.

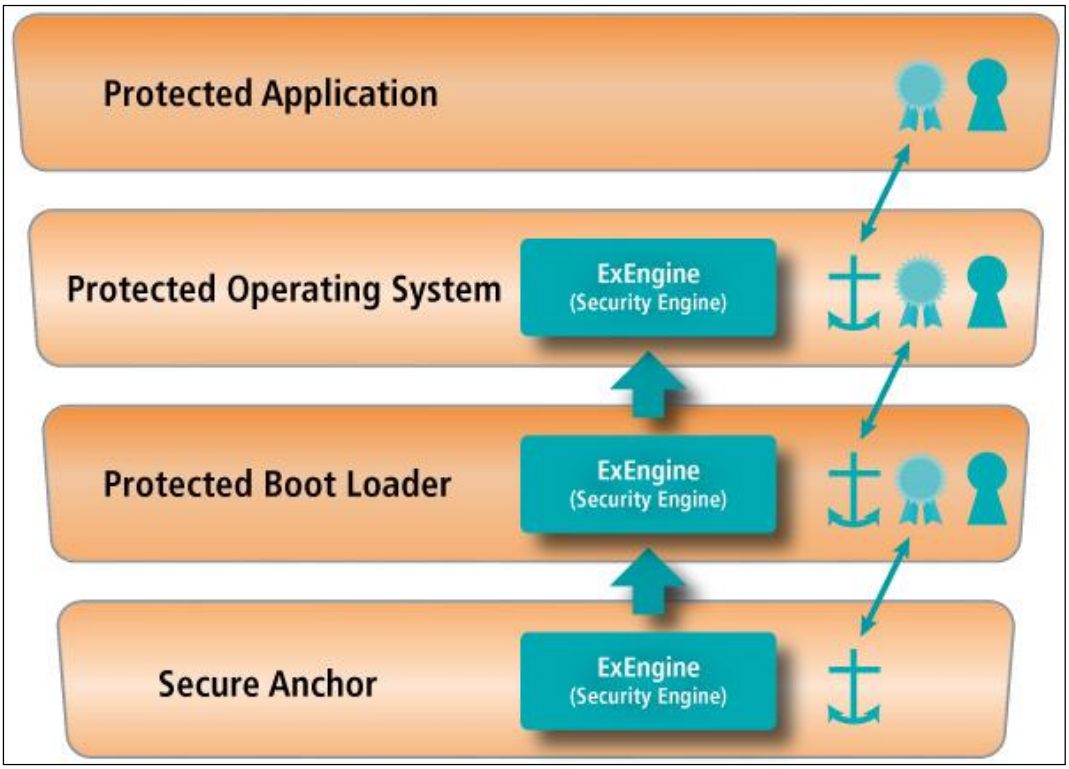
All cryptographic processes make use of industry standards like Advanced Encryption Standard and elliptic curve cryptography. Both algorithms are supported natively by the smartcard controller.

RESULTS

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

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 (extensible to -40°C to 105°C) typical of industrial applications.



ABOUT 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.

About Infineon Technologies AG

Infineon Technologies AG is a world leader in semiconductor solutions that make life easier, safer and greener. Microelectronics from Infineon is the key to a better future. In the 2014 fiscal year (ending September 30), the company reported sales of Euro 4.3 billion with about 29,800 employees worldwide. In January 2015, Infineon acquired US-based International Rectifier Corporation with revenues of USD 1.1 billion (fiscal year 2014 ending June 29) and approximately 4,200 employees.

Addressing the need for security in an increasingly connected world is the charter of Infineon. Infineon is the leading provider of security solutions and offers tailored and ready to use security solutions serving a wide range of applications from smart cards to new, emerging use cases. Outstanding security expertise and technology innovation based on almost 30 years of experience, system competence and the broadest security solution portfolio focused on customer needs is what makes Infineon the preferred security partner. Visit www.infineon.com/ccs

In October 2015 Infineon has launched the Infineon Security Partner Network. This is a place for security players to deliver security solutions to providers of connected devices and applications. This network conveniently enables system and device manufacturers to understand security needs in the context of their application and offers tailored support for the implementation and deployment of security solutions. Visit www.infineon.com/ISPN

About the Industrial Internet Consortium

Wibu-Systems and Infineon Technologies are both members of the Industrial Internet Consortium (IIC). The Industrial Internet Consortium is a global public-private organization of over 210 members, formed to accelerate the development, adoption and wide-spread use of interconnected machines and devices, intelligent analytics, and people at work. Founded by AT&T, Cisco, General Electric, IBM and Intel in March 2014, the Industrial Internet Consortium catalyzes and coordinates the priorities and enabling technologies of the Industrial Internet. Visit www.iiconsortium.org.