Press Release – 6 April 2017

Securing microcontrollers in unsecure connected environments

Bronze Podium for CodeMeter µEmbedded at the Electronic Product of the Year Awards 2017

Karlsruhe, Germany – CodeMeter µEmbedded, the Wibu-Systems' CodeMeter variant made especially for software developers to protect application code and intellectual property against reverse engineering on microcontrollers and Field Programmable Gate Arrays, has taken the third place in the annual Electronic Product of the Year competition led by the German publishing group WEKA. The award ceremony that took place on March 31st was the final highlight of a selection process in which the editorial team of Elektronik screened all of the most recent innovative and forward-looking products and left their readers the final vote from among 111 picks.

An increasing number of systems in the professional and consumer markets is managed by microcontrollers. These units use sophisticated algorithms and likely need firmware updates during their lifetime. The firmware of today's microcontrollers is generally loaded onto controllers as a compiled hex image using a serial connection, without any protection against reverse engineering or fraudulent manipulation. This leaves the file vulnerable in its transfer from the build system to the controller and jeopardizes the trustworthiness of the end-to-end production process.

Even if the manufacturer trusts his own build process, the microcontroller is no longer located in a controlled environment after it has left the production site. Vendors thus face a double threat: product know-how stolen by competitors and tampering attacks during updates and upgrades of the firmware. Either can occur in any insecure and unpredictable environment regulated by end users.

To achieve a comprehensive solution that meets the goals of know-how protection, integrity protection, and license-based monetization, the firmware (of an Infineon XMC™ microcontroller in this case) is encrypted by CodeMeter µEmbedded with symmetric and asymmetric (AES and ECC) algorithms, digitally signed as part of the build process in DAVE™ (Digital Application Virtual Engineer) toolchain and uniquely bound to the microcontroller.

During the third-party production of a XMC4500-based device, the secure firmware is loaded into the controller. When powering up for the first time, the loader communicates with the production system, generates a fingerprint of the device, and is injected with a license. From then on, only encrypted, licensed, and signed firmware can be loaded into the XMC microcontroller. If needed, the firmware can also use the license information for custom behaviors. The firmware cannot be extracted from the XMC, and it is read-protected by internal XMC mechanisms.

To bolster security further, it is possible to extend the hardware binding to an external secure element like an OPTIGA™ TPM (Trusted Platform Module) or an SLE security controller communicating via Serial Peripheral Interface (SPI) with the XMC controller.

Oliver Winzenried, CEO and founder of Wibu-Systems, sees the security of microcontrollers as the lifeblood of modern technology “We have the interests of all software developers at heart; regardless of the platforms or systems they have specialized in, our CodeMeter technology has a flavor to address the needs of computers, mobile devices, embedded systems, PLCs, and even microcontrollers. Their computational power and performance vary considerably; still, we have managed to provide the backbone of our security capabilities in

just 60 kBytes for the loader code. But even more significantly, we ensure complete compatibility in between all the CodeMeter variants, so that heterogenous landscapes can be protected and licensed with the same technology and considerable savings in the investment made."

Wibu-Systems' CodeMeter µEmbedded wins the Electronic Product of the Year Award 2017 © Horacio Canals

Press contact at Wibu-Systems
Daniela Previtali, Global Marketing Director
Tel. +49 721 9317235 / +39 035 0667070
daniela.previtali@wibu.com, www.wibu.com

WIBU-SYSTEMS AG (WIBU®), a privately held company founded by Oliver Winzenried and Marcellus Buchheit in 1989, is an innovative security technology leader in the global software licensing market. Wibu-Systems' comprehensive and award winning solutions offer unique and internationally patented processes for protection, licensing and security of digital assets and know-how to software publishers and intelligent device manufacturers who distribute their applications through PC-, PLC, embedded-, mobile- and cloud-based models.

Media graphic resources available at: http://www.wibu.com/photo-gallery.html