NEWS & INSIGHTS FROM THE WORLD OF ID SECURITY

JUNE 2018

The VAULT

USING DNA LEARNING TO CREATE AN "INTEGRITY GUARD"

TECHNOLOGY

Who controls the controllers?

IT Security for the car of the future

Mobile security from Infineon

INSIGHTS

Interview with Infineon's Thomas Rosteck

Financing models for eID projects

Who CONTROLS the *CONTROLLERS?*

By Daniela Previtali, Wibu-Systems

Think product piracy is a matter for music bootleggers or knock-off designer handbags? Think again: Theft, sabotage, reverse engineering, and other attacks on legitimate business are affecting all sectors of the economy. As the most recent data from the German engineering association VDMA reveals, the threat of product piracy shows hardly any signs of abating.

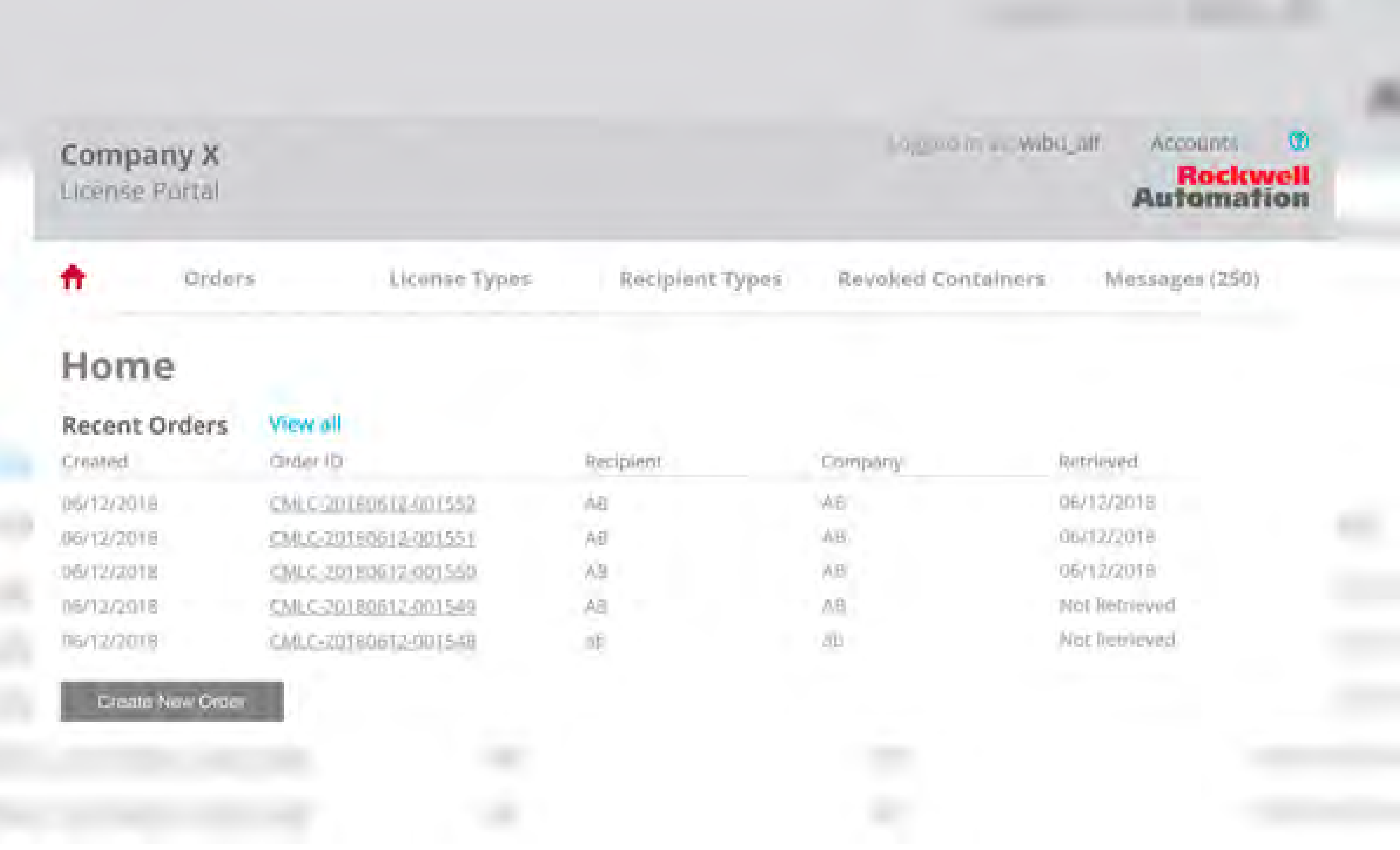
While the problem does not seem to have become more prevalent, the number of companies victimized by product pirates remains at historically high numbers. And the nature of the threat is changing: As more and more product features and properties are moving into the softer realm of looks and designs or software and operating systems, many would-be pirates can ignore the difficulties of copying complex proprietary hardware. Their targets are now more intangible in nature – software code, product specifications, or machine operating systems – and their preferred line of attack is now digital.

□ Companies invest untold hours of work and vast sums of money into their products long before they can ever hope to reap a return on their investment. At every stage in that long journey from the drawing board to the finished product, their intellectual assets are at risk of being lost, by inadvertent leaks or malicious action. What the intelligence services term human intelligence – using human actors as sources of information – will always remain a soft spot in the economy, as former or current employees, retailers, service personnel or many others can be leaned upon or otherwise incentivized to pass on confidential information. With the industrial world moving increasingly to the connected, digital realms of smart factories and "Industrie 4.0", new threats are appearing at other links in the chain: The endpoints and lynchpins of connected industrial systems.

Hardening the Industrial Landscape with Rockwell Automation

Rockwell Automation, the Fortune 500 listed maker of industrial automation solutions, has turned to Wibu-Systems to combat these new threats with robust protections in Rockwell Software Studio 5000 Logix Designer. Its solution, License-Based Protection, is based on the CodeMeter technology to encrypt and decrypt the code to run on the systems with dedicated licenses, that allow full control over which functions can be accessed where, when, and by which users.

The process is simple, but robust: the source code of Rockwell Software Studio 5000 Logix Designer is encrypted and protected by separate licenses for separate features. Similarly, the code to be executed on Rockwell's PLCs Allen-Bradley-ControlLogix 5580, CompactLogix 5380, and CompactLogix 5480 is encrypted. The users are equipped with dedicated master keys to create their very own licenses according to the functions they need, allowing system developers to work freely with the specific modules they have been entrusted with or maintenance professionals to test unencrypted functions, monitor machine performance data, or upload secure updates. Time-based licenses can even set specific expiry dates to restrict the window of time even further in which the system has to let its guard down. With full control over the licenses and encryption keys, the system is sealed off against manipulation through the



Company X
License Portal

Logged in as: wibu_alf Accounts

Home

Recent Orders View all

Created	Order ID	Recipient	Company	Retrieved
06/12/2018	CMLC-20180612-001552	AB	AB	06/12/2018
06/12/2018	CMLC-20180612-001551	AB	AB	06/12/2018
06/12/2018	CMLC-20180612-001550	AB	AB	06/12/2018
06/12/2018	CMLC-20180612-001549	AB	AB	Not Retrieved
06/12/2018	CMLC-20180612-001548	AB	AB	Not Retrieved

back door. On the shop floor, the user will experience these new protections mostly in two of their specific expressions: CmDongles and a dedicated Web Portal.

Built for Ease in the Real World

CmDongles are a specialized piece of secure hardware which act as a physical token of authorized users. Different form factors are supported, i.e. CmStick/M, CmStick/C, or CmCard/SD. What they all have in common is their inclusion of an Infineon smart card chip as the backbone of their encryption capabilities. Symmetric and asymmetric AES (Advanced Encryption Standard), RSA (Rivest-Shamir-Adleman), and ECC (Elliptic Curve Cryptography) encryption are available, and Infineon has secured its chip against side channel attacks to make the secure hardware itself truly manipulation and tampering-proof. For communication, CmStick/M and CmStick/C can be configured as human interface devices (HID) to work even in environments that need to ban regular USB for security reasons, as is common in many industrial environments. CmCard/SD includes 4 GByte additional SLC flash memory on top of the regular 328 kByte provided by the smart card chip to store licenses and entitlement rights of single or multiple vendors.

In order to get the licenses they need onto their CmDongles, the users of Rockwell Automation's new solution use the Web Portal as the front end of CodeMeter License Central provided by Wibu-Systems. The portal manages and allocates the licenses and entitlements for both the source code and the actual operating code. When work needs to be done on a specific machine, the portal can be used to assign the rights to a developer or maintenance technician, with preset user profiles available for different levels of protection, e.g. limiting access to source code to authorized engineers or allowing access only for a specific window of time. The web portal makes easy work of coordinating these rights with full control over license types, recipients, user profiles and other granular license information.

> *“With license-based protections, the makers of automation solutions and the operators of smart factories are stopping the constant stream of manipulation, reverse engineering, or hacking attacks in their tracks.*

More Protection Pioneers

Rockwell Automation is not the only leading maker of industrial automation solutions to avail themselves of the security powerhouses made by Wibu-Systems and powered by Infineon’s cryptocontrollers. The 14th version of Siemens’ Totally Integrated Automation (TIA) Portal relies on CmDongles as safe repositories of the passwords needed to access the highly confidential data on the system. The versatile password management tool makes it easy for passwords to be created and assigned offline or online, to suit the security needs of the user. As the passwords never need to leave the secure environment provided by the CmDongles, their users can access the engineering projects and the data they are entitled to, safe in the knowledge that their rights cannot be compromised.

Other pioneers of industrial automation are also following suit. B&R also opted for CodeMeter to secure their Automation Studio development tools and the runtime of the automation computers in the field; each unit is provided a CmStick that protects the most valuable digital asset – the source code of B&R’s automation technology – while also giving the user more freedom with CodeMeter’s multi-vendor capabilities. The CmSticks are not limited to carrying B&R’s own licenses, but also licenses from other vendors to handle third-party components in the often heterogeneous landscapes of modern connected factories.

Enabled™ by
Rockwell Automation
Technologies

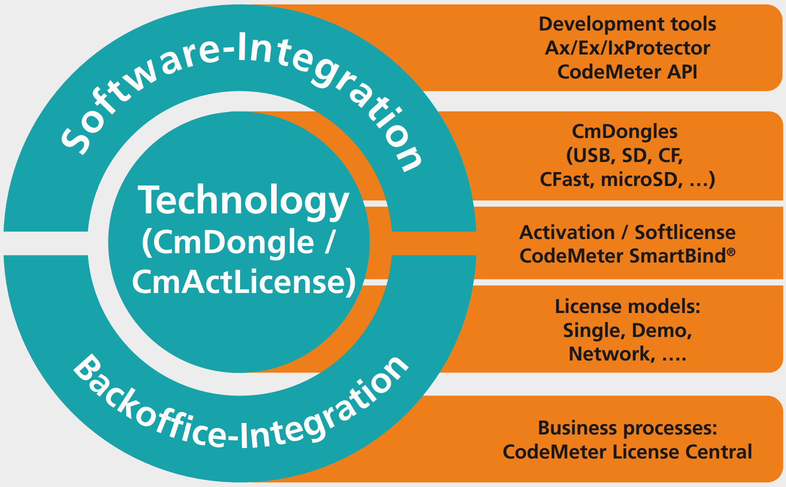
With license-based protections, the makers of automation solutions and the operators of smart factories are stopping the constant stream of manipulation, reverse engineering, or hacking attacks in their tracks. Not only are they ramping up the level of protection at the essential core of automated industry; the new licenses also give them and their users much more granular control over the way their products and technology are used on the ground – feature by feature and user by user. ☒

CodeMeter stands up for Industrie 4.0

WIBU SYSTEMS

CodeMeter for Industrie 4.0 – Watch the full Video – www.wibu.com/40

New business models for software publishers and device manufacturers


Software-Integration

Technology (CmDongle / CmActLicense)

Backoffice-Integration

Development tools
Ax/Ex/IxProtector
CodeMeter API

CmDongles
(USB, SD, CF, CFast, microSD, …)

Activation / Softlicense
CodeMeter SmartBind®

License models:
Single, Demo, Network, ….

Business processes:
CodeMeter License Central

In its mission to deliver the most secure, unique, and versatile technology, Wibu-Systems has developed CodeMeter®, a comprehensive, award-winning suite of hardware and software solutions for **computers, embedded systems, mobile devices, PLCs, and microcontrollers** that incorporates internationally patented processes dedicated to protecting the integrity of digital assets.

With its motto **"Perfection in Protection, Licensing, and Security"**, Wibu-Systems supports ISVs and OEMs in their fight to **safeguard the intellectual property** of their applications against illicit and fraudulent use, reverse engineering, tampering, sabotage, espionage, and cyber-attacks, while generating new **software-feature based business models** fully integrated with ERP, CRM, and e-commerce platforms.

The unparalleled lineup of **hardware secure elements** (USB dongles, SD cards, microSD cards, CF cards, CFast cards, ASICs) designed to withstand high fluctuations in temperature, humidity, and vibration, coupled with the support of all mainstream operating systems and M2M communication standards makes CodeMeter the ideal candidate for both **brown and green field** applications.

//CODiE//
2017 SIIA CODiE WINNER

SECURITY
LICENSING
PERFECTION IN PROTECTION

www.wibu.com | sales@wibu.com | +49 721 931720