NEWS & INSIGHTS FROM THE WORLD OF ID SECURITY

JUNE 2017 | #20

The VAULT

APPLICATIONS
Airport - the future of Checkpoint Delta
Authentication - bridging the credentials gap

TECHNOLOGY
A new encryption paradigm
Virtual token - a smart card alternative?

INSIGHTS
De La Rue on Next generation ID
Bringing IoT securely into the developing world

NEXT GENERATION IDENTITY SOLUTIONS

A NEW *Encryption Paradigm* for a NEW INDUSTRIAL AGE

By Daniela Previtali, Wibu-Systems

Long before encryption became a commonplace feature of even consumer computers, while computers were still mechanical contraptions and encryption the domain of military cipher clerks, Auguste Kerckhoffs published two articles on the subject in the “Journal des sciences militaires” in 1883. He proposed several principles, one of which remains fundamental for modern cryptography: “The system should not require secrecy, and it must not be a problem if it falls into enemy hands.” Put more simply: Let the enemy know the system, as long as they don’t know the key!

□ In essence, the dictum that became known as Kerckhoffs’ Principle states that the strength of the encryption system should depend on the key being used, not the secrecy of the system. The system can and should be public knowledge. Even if the enemy, be it a military adversary of yesteryear or a modern software pirate, can access it, he would still lack the key to break it. At the same time, it is also open for researchers to analyze, challenge, and make it stronger.

Even now, more than a century after Kerckhoffs proposed his eponymous principle, most security depends on keeping the systems hidden from the public. “Security by obscurity” is the much-maligned, but still widely followed paradigm in the software industry and beyond. Maintaining secrecy about the technology has its advantages, and even strict adherents of Kerckhoffs do not suggest that all encryption mechanisms needs to be laid bare. Still, an approach that puts all of its trust in secrecy cannot be independently verified: Security by obscurity also means an obscure level of security.

> *“An approach that puts all of its trust in secrecy cannot be independently verified: Security by obscurity also means an obscure level of security.”*

What makes a system truly secure?

For us to know whether a system is secure, two factors need to be present: The security property needs to be described precisely, and it must not rely on assuming many restrictions on the attacker. An attacker might not only have access to the encrypted text, but also the plaintext, or he might be able to interfere with either end of the communication, as happened in the famous case of the captured Enigma machine. While the system – the rotors – was a closely guarded secret, the code breakers at Bletchley Park managed to crack it, because they knew part of the plaintext – tiny bits of the message they had guessed correctly.

True security depends on encryption whose strength is mathematically provable, not conjectured by trust in an obscure system. To be demonstrably “hard to solve”, it has to become exponentially more difficult as its scale increases. Today’s 2048-bit encryption is virtually impossible to crack with the current limits on computational power. Modern encryption systems should be published with demonstrable security properties of this nature, and by fact of being published, they are open to being validated or indeed invalidated. This makes them truly Kerckhoffs-compliant.

Laying open the Blurry Box

For Industry 4.0, strong encryption can have make-or-break impact, opening entire new business models and revenue streams or exposing intellectual property and business-critical data to hackers, pirates, or saboteurs.

> *“For Industry 4.0, strong encryption can have make-or-break impact, opening entire new business models and revenue streams or exposing intellectual property and business-critical data to hackers, pirates, or saboteurs.”*

Wibu-Systems has pioneered the Blurry Box technology with this need in mind, fully compliant with Kerckhoffs’ Principle and demonstrably hard to solve. The essence of Blurry Box encryption lies in how it handles the function blocks that constitute a piece of software.

Blurry Box splits each function block into several variants, which return the correct output of the original unencrypted function only for a specific input set. A wrapper function maps these inputs to the variants, which are encrypted with separate keys stored on a dongle. When the software is executed, the system only decrypts those variants that match the given input. Hackers will only ever see that part of the code that matches the previous input.

In traditional encryption, hackers could work their way through the function blocks in what is called a copy-and-paste attack. However, even if a hacker captures individual variants, the principle of inherent complexity demands that the protected program is so complex that no hacker can derive additional variants from a specific subset that may become known to him. In essence, Blurry Box does not depend on making copy-and-paste attacks on individual variants impossible, but on making the attack strategy as a whole unfeasible.

Special traps are included should an attacker attempt to simply force his way through the variants. Once triggered, the trap locks the dongle, which also happens when illegal sequences are detected. This stops hackers from simply retracing a few steps without running the entire process (with the effort and complexity this entails) from the beginning.

Made for Industry 4.0

Blurry Box encryption has great potential for Industry 4.0 environments. The rise of the interconnected industry has created many tempting targets for cyber-attackers wishing to cause damage or steal know-how. The situation is already alarming: According to the Product Piracy Study 2016 published by the German engineering federation VDMA, 9 in 10 industrial machine manufacturers have already fallen prey to pirates.

Preventative measures against these naturally include encryption, as showcased at the demonstration platform SmartFactoryKL, where innovative connected manufacturing technologies are tested with secure communication, using cryptographic keys stored in secure elements. Invaluable data like product designs or machine settings are digitally signed and stored on RFID tags and verified via the cloud. The machines cannot be tampered with and only accept data from authorized sources. The new controls are a boon for sectors of the market heavily affected by product piracy or the revenue-depleting competition of the grey market, like the fashion industry.

Many modern IoT devices are reliant on microcontrollers to deliver their functions. Their makers can include protection mechanisms in their development toolchain and secure their firmware to prevent later tampering or enable such commercially indispensable features as production volume controls, secure updates, or the remote activation of add-on features.

This creates new after-sales potential and allows for completely new business models.

The potential of secure protection and licensing is not limited to the manufacturing industry. Many other sectors are experiencing a shift from hardware-dependent to software-realized functionalities: Innovative medical technology firms are beginning to offer their devices at low entry prices, giving medical professionals in the emerging markets and smaller healthcare facilities everywhere access to cutting-edge therapeutic and diagnostic equipment. They can then offer add-on functions as paid upgrades or with pay-per-use schemes. All this is made possible, secure and fully compliant with the strict standards in the industry, by a sound licensing system.

"Many modern IoT devices are reliant on microcontrollers to deliver their functions. Their makers can include protection mechanisms in their development toolchain and secure their firmware to prevent later tampering or enable such commercially indispensable features as production volume controls, secure updates, or the remote activation of add-on features."

Conclusion

An encryption mechanism that is true to Kerckhoffs' Principle represents a genuine seismic shift away from deceptive "security by obscurity" towards genuinely open, but strong protections. The secure and flexible licensing and encryption capabilities provided by Wibu-Systems are a game changer in the field.☒

Global Hacking Competition

In the true Kerckhoffs' spirit, Blurry Box effectiveness and methodology are being tested in the field. At the opening of the Hannover Messe, Wibu-Systems has called all hackers around the world to crack an application protected with Blurry Box. Results will be made available at www.blurrybox.com.

BLURRY BOX

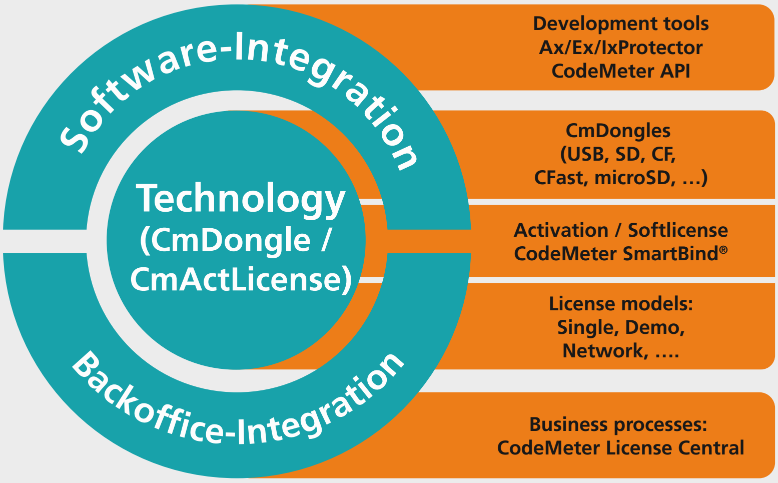
CodeMeter
Securing the Industrial Internet

WIBU SYSTEMS

- Industrie 4.0
- Smart Factories
- Embedded World

CodeMeter Security – Watch the full Video – www.wibu.com/cms

New business models for software publishers and device manufacturers



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.

5. Deutscher IT-Sicherheitspreis 2014

SECURITY
LICENSING
PERFECTION IN PROTECTION

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