Security has more dimensions than just crypto algorithms!

By Marco Blume, Wibu-Systems

This article highlights CodeMeter Embedded 2.0 which comes packed with new features and abilities and can now access key storage with multiple processes. This might not sound like a great deal, and it has long been standard on desktop PCs, but it has to date not been possible on embedded systems.

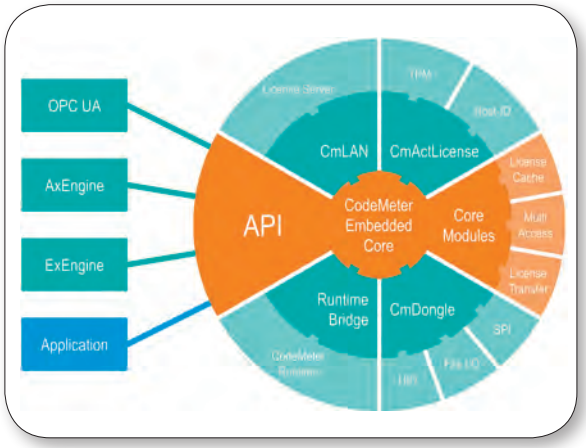

Figure 1. CmEmbedded 2.0 includes now License Core which allows the integration of additional software components.

■ CodeMeter is far more than dongles for protecting software – CodeMeter is a complete solution, an entire universe of components from development tools to the integration of license creation into sales processes. Crypto libraries are just one part of the edifice. Many providers have come up with AES encrypted software code and integrity protection mechanisms based on elliptical curves (ECC). They are on the right track, and their technology is absolutely state of the art. CodeMeter is also based on it, but it does not stop there: the best encryption algorithms are immediately useless whenever the keys are not stored securely as well. And even if the keys are kept secure in a Trusted Platform Module (TPM), the problem is only half-solved. How do they get there? Can they still be updated after 10 years of service in the field or when the system is offline? Is the system still as secure as it should be? How can developers and clients keep track of their keys on all their devices? All these vital questions can be solved, as we will prove.

On top of protecting the invaluable know-how of developers, businesses have another important goal: to earn money with their devices or software. This monetization essentially means enforcing some form of licensing system. To do so, the software needs to be protected from illicit use, closing the circle and taking us back to encryption. Beyond preventing or allowing a software to be run (i.e. decrypting it), licenses can have many other features. They might limit the duration or number of times a software can be used. They can contain protected data, like operating parameters. Additional licenses can be used to unlock add-on features. Of course, licenses can be tied to a specific system to stop illicit copying. Everything works together – CodeMeter users get know-how protection and the opportunity to introduce versatile licensing concepts that might open up complete new business opportunities.

Scalability to serve all systems

CodeMeter scales from servers and workstations, via the entire universe of different embedded systems, down to the tiniest microcontrollers. A fast-growing type of computer is entering our lives, not the old box on people desks, but tiny computers built – embedded – into other devices or machines. CodeMeter Embedded (CmE) is the CodeMeter version for embedded systems like industrial controllers or mobile devices, i.e. for anything that is neither a traditional PC or laptop or a server in a rack. This means that CmE serves the market that uses 98% of all computer processors produced today. At the lower end of the scale, where FPGAs and microcontrollers start, the baton is passed on to CodeMeter µEmbedded. It is designed with even smaller systems in mind, while staying fully compatible with the licenses and infrastructure of the greater CodeMeter universe.

CmE has been around for several years. As the needs and expectations of users have increased and the systems have become more powerful in terms of computational power and storage space, the feature set has also evolved. It runs on all major platforms like x86, ARM, and PPC and virtually on any operating system. The automatic software protection features of AxProtector are available for Linux, Android, and Windows. Integration with VxWorks does even further, and the features can be accessed directly with the tools of Wind River and used in a secure boot process in cooperation with an UEFI. For other systems, CmE is available in source code, allowing clients to use it in special real-time operating systems or bare-metal implementations (directly on the hardware without any operating systems).

Secure Key Storage

Put simply, CmE is the agent working between protected applications and key storage. It behaves not unlike a driver:it gives the protected program an API for executing cryptographic operations, updating licenses, or storing data securely. On the key storage side, it supports different types of storage and handles them transparently for the API – again

Figure 2. CME 2.0 can be used on a variety of hardware components.

reminding us of how drivers work. The crypto API is only part of the solution. The keys need to be securely stored as well to achieve true security. In the CodeMeter universe, this can be done on a piece of hardware or in a file. Hardware in this case means a secure element – a specially customized chip that stores all the secret information well away from prying eyes. Cryptographic operations are executed on the chip itself, and the keys never need to leave their secure home. Only the results of the operation are returned to the outside world. This is the strongest form of security, and it is used in a similar form in cell phone SIMs or TPM chips. The hardware secure element can come in many shapes and sizes, from USB dongles or microSD cards to ASICs that communicate with the system via an SPI interface. If hardware is not an option, the software solution, a CmActLicense, provides the same functions as a dongle. The only difference is that the cryptographic operations will not happen in a dedicated piece of hardware, but on the protected system itself.

The CmActLicense file remains protected and is tied to several unique traits and markers of the host system to prevent it from being copied. Another secure option for storing keys is to rely on networked CodeMeter servers that can supply several devices with the licenses they need, without each device having an individual license installed. The necessary communication is again protected with changing transport keys to prevent wiretapping and manipulation. For the CodeMeter API, all of these variants are fully transparent and can be mixed and matched as needed, since all key storage options are designed to be compatible with each other.

License Lifecycle Management

The second challenge remains: how to get the keys and licenses into their container? This is again a more complex operation than a simple key transfer – the licenses need to be sold, created, and managed correctly. This is made easy with a simple tool called CodeMeter License Central. Like the other solutions, it has been developed to scale perfectly from handling single user licenses on a few individual computers, with licenses created manually, to small-scale online shop operations and even large corporate ERP systems, with dependable high-availability hosting in any given data center. In CodeMeter License Central, individual licenses are created for each target device. The update files that contain these licenses can be transferred by virtually any medium, as they are encrypted and tamper-proof. They can only be decrypted in the specific target container, be it a dongle or a CmActLicense. The same mechanism can be used to license additional add-on functions after the original sale or to renew licenses limited to a specific duration or volume. In the same manner, trial licenses can be upgraded to full licenses.

Automatic Encryption Processes

AES encryption is known to be secure. If anything is cracked, the problem usually lies in a poor implementation, not in the AES algorithm itself. Wibu-Systems want its customers to concentrate on what they do best. That is why the CodeMeter Protection Suite gives them a powerful tool to take over the task of encrypting and protecting applications or libraries. Developers can protect the software they have completed without knowing anything about encryption and directly activate the licensing system. CodeMeter Protection Suite does the heavy lifting for them: encrypting the software, integrating the decryption tools, and adding the meta-data – a great tool and the product of over a quarter of a century of experience in software protection.

CodeMeter Embedded 2.0 vs CmE 1.0

Why choose CodeMeter Embedded 2.0? Because it comes packed with new features and abilities. CodeMeter Embedded can now access key storage with multiple processes. This might not sound like a great deal, and it has long been standard on desktop PCs, but it has to date not been possible on embedded systems. The code was meant to be as lightweight as possible, it should not have any services running, and CmE was to be a directly integrated part of the encrypted program. The advent of more powerful embedded systems, however, brings new capabilities, which means that several protected programs and processes could share access to a single CmContainer. Changes to the inner workings have made the licensing system more flexible and effective. We are calling it License Core. The new functions allow the integration of additional software components. Based on License Core, an OPC UA stack can now be used with CodeMeter as key storage. Updating CodeMeter licenses is now also possible via the OPC UA protocol.

By relying more on secure elements in chip format that are built into new hardware already in the design stage, the SPI interface is integrated to handle communication. This avoids the detour via the USB stack, saves energy, and accesses the chip directly. CmE 2.0 is putting down the groundwork for the license transfer feature introduced in the desktop version in 2016. The new functions will be supported in embedded systems as well as new functions and features are being rolled out. CmE will never be a run-of-the-mill product – many of its features are designed to be modular. The mission has been and still is to produce the most compact software possible.

That is why we first ask new clients about their target system and use case before we produce the right package for them. This means that CmE can scale to match the client's needs. It is never a monolithic block of deadweight on the system resources. Wibu-Systems today offers a licensing and protection solution for almost any device that contains a processor. We are supporting developers with the implementation and sales professionals with the management of their licenses. ■