https://eetimes.eu/the-need-for-security-technologies-for-embedded-electronics/

EE Times EUROPE

The Need For Security Technologies For Embedded Electronics

October 31, 2019 Maurizio Di Paolo Emilio

IoT is an ecosystem that will evolve all our industrial sectors through a digital transformation. The world around us is already changing. We think of the agricultural sector, city infrastructure, retail, and the automotive industry with new embedded solutions. Security is one of the most critical aspects to manage, and often it happens that embedded devices, especially the small ones, are lacking even the minimum necessary protection requirements.

Embedded systems achieve very high functional complexity, especially when they are based on highly integrated core processors. The developer is faced with high functional complexity and a series of application requirements for the development of the system firmware, as well as to guarantee deterministic, safe, and real-time behavior.

The most important change in security will come from the fact that the IoT will become more rooted in our lives. Concerns will no longer be limited to protecting information and sensitive assets. Our own lives and health can become targets of hacking attacks.

In the embedded world, safety and security concepts are closely connected. The security essentially concerns information and, therefore, is aimed at fighting attacks by malicious actors; safety, on the other hand, concerns the safety of people and the protection of tangible assets.

Behind all this, the importance of securing the entire IoT ecosystem is very important. The industry is in its state of digitization, where each vendor hastily tries to distribute the next innovative device connected before the competitors do. In these circumstances, functionality becomes the main objective, and security takes second place.

The future of IoT will also depend very much on the decentralization of the networks by moving some activities towards edge or fog computing with the use of innovative business models in mission-critical operations.

Wibu-Systems wants to offer the highest level of protection, licensing and security for digital assets and intellectual property in an increasingly connected world. With Daniela Previtali, Global Marketing Director at Wibu-Systems, the essential security aspects of the IoT embedded world will be addressed.

EET: Wibu-Systems is an innovative security technology leader in the global software licensing market. What's the market where you are pushing substantially? Could you describe your latest updates briefly?

One of our principal innovations is our commitment to what we call 4D interoperability. Everything works with everything else: Software, hardware, and cloud containers, computers, mobile units, embedded devices, PLCs, microcontrollers, and FPGAs, different operating systems and architectures, and everything fully integrated with common back-office solutions and business processes.

We make significant investment in cross domain integrations because our markets are just as diverse. There is intensive effort going into medical equipment, industrial automation, machine vision, AI, and 3D printing, but just as much attention paid to gaming and gambling, finance, media, and virtually any other software powered market segments.

All these applications fuel our constant innovations, starting with our new industry-grade CmDongles with USB type-C connectors and MLC or pSLC flash memory.

Data protection in networked environments is a major issue, which is why we introduced CodeMeter Certificate Vault as the perfect solution to deploy certificates via CodeMeter License Central on CmDongles and use them with PKCS#11, Microsoft CNG (Microsoft Cryptographic API Next Generation) or OpenSSL. They provide a secure machine identity in OPC UA based M2M communications. Private keys are stored in the smart card chip onboard the CmDongle; they never leave the safety of the hardware and they can be used for cryptographic operations like digital signatures and encryption.

The next step is protecting the data and the software itself. Data is currency for the developers and users of modern PLCs. We have a toolbox with cutting-edge encryption methods for Windows, Linux, Android, macOS, .NET, Java, and the embedded world, as well as CodeMeter-derived solutions specifically for the users of CODESYS, Studio 5000 Logix Designer, or the TIA Portal to protect sensitive code (source protection), while enjoying all the benefits of complete license lifecycle management. Machine builders that want to license a growing number of features on controllers as they embrace Industry 4.0 principles can also rely on the same tools they receive from PLC vendors to realize robust execution protection and customer-centric monetization mechanisms.

The most recent innovation is CmCloud, which takes our tried-and-tested protection and licensing technology into the cloud. In industry, PLCs are often connected to the cloud via a gateway as a handy means for selling and distributing analytics and predictive maintenance services. These services are provided from the PLC vendor to the user via the cloud. They need licensing, as this is where CmCloud comes into play with our ability to sell services through licenses with different license metrics, such as the number of devices, or pay per usage, or maintenance periods.

There are still many scenarios where security considerations or simply the legacy conditions on the ground prohibit 'always-online' setups. For PLCs that are not connected to the Internet, licensing used to be a cumbersome effort, and the license updates needed for modern monetization models like usage counters or features-on-demand were near impossible. We have streamlined that process with our CodeMeter License Central portal and provided a secure way of transferring license updates physically into devices out in the field (figure 1).

Figure 1: CodeMeter Certificate Vault

EET: The digitalization of our society has far-reaching implications. The urgency for viable security solutions grows day by day. What's the impact of data security in all industry 4.0? What do we need to do to secure the IoT and IIoT?

Data security is the very essence of Industry 4.0. It actually means two separate, but interlinked, aspects: Identities and data. Both are key for man-machine interactions, but even more for M2M communications, which usually happen automatically and with very little oversight from human operators. Long before anyone even notices a technical issue, the damage might already be done, so the entire system needs security by design and by default.

Consider identities from the point of view of a modern connected medical device in hospital: As the operator, you want to know the device you are using on your patient is the original article and not a back-alley fake. Second, the device needs to know your instructions are genuine and come from a certified controller.

Now consider data, which again comes in two forms. There is configuration data, which includes the practical settings, but also the underlying operating software. You need to know that nobody has tampered with the inner workings of our hypothetical medical device, potentially holding patients' lives as ransom.

Finally, there is the operating data that makes up most of the data flowing through our connected world. In our example, it could be patients' medical files with all the confidentiality concerns that it entails. Or it could be 3D print designs, patterns for new garments sent from a couture designer in Paris to workshops in Asia, or any other form of the data that has become the currency in the IIoT.

CodeMeter not only protects both types of data. It goes further and allows you to monetize it via smart licensing: e.g. you can control how often a device can be used or even upsell add-on features.

EET: What future challenges do you see affecting embedded security, and how do you plan to evolve your suite of products to meet those challenges? Which technical aspects should be considered by an embedded designer for a software (but also hardware) point of view?

The world around us is getting more diverse every day, and the digital world is following suit: The hegemony of single platforms is a thing of the past, as developers have a vast array of hardware and software options to choose from, not to mention the endless variety of endpoints and devices making up the Internet of Things.

One of the main design principles for our CodeMeter Protection Suite has always been compatibility: It can handle many different processor platforms and operating systems, complemented by a powerful API. The essence of IP protection, feature licensing, and security, i.e. integrity protection, holds true, independent of the target system. Supporting so many platforms and engineering tools is a major challenge, but we stand by our commitment.

Embedded designers need to understand the security challenges and threat scenarios for their application to select the right security concept. Piecemeal proprietary solutions for each and every software product or endpoint are a virtual invitation for cyber-attacks, as the chain is only ever as strong as its weakest link. And they are a nightmare to run without hobbling the business with their sheer complexity. CodeMeter fits virtually every use case and does not inhibit, but actually helps with monetization, but it is about far more than

designing or choosing a single security component. Businesses need to see security holistically, which is why our Professional Services team is here to help them by contributing their unique systemic viewpoint (figure 2).

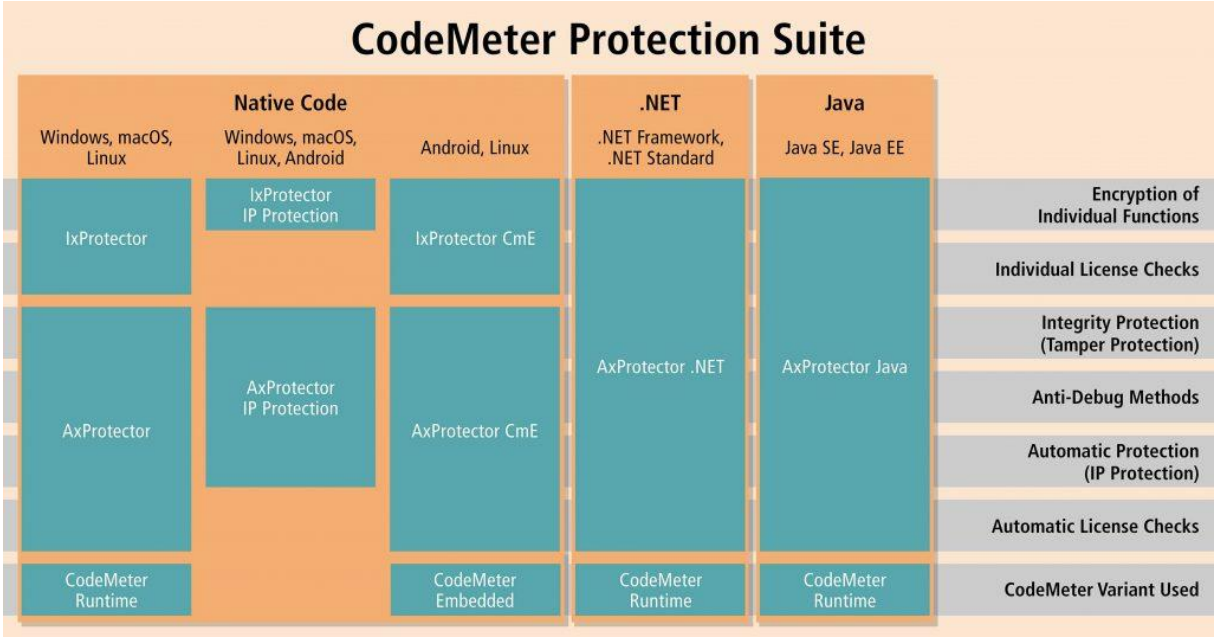

Figure 2: CodeMeter Protection Suite

Maurizio Di Paolo Emilio

Maurizio is an Electronic Engineer with a Ph.D in Physics. Maurizio enjoys writing and telling stories about technology and electronics. His main interests are Power, Automotive, IoT, Digital. Maurizio is currently editor-in-chief of Power Electronics News and European Correspondent for EE Times. He also oversees discussions on EEWeb.com.