Embedded security rises and falls with crypto key management

Stephen Evanczuk - December 02, 2014

This article is part of EDN and EE Times’ Hot Technologies: Looking ahead to 2015 feature, where our editors examine some of the hot trends and technologies in 2014 that promise to shape technology news in 2015 and beyond.

Embedded systems face ongoing threats of penetration by persistent individuals and organizations armed with increasingly sophisticated tools. On-chip security features do serve as fundamental enablers for secure systems but can provide a false sense of security without a broader view of security policies. Consequently, the trend toward enterprise-level security lifecycle management emerges as the most promising solution for hardened security in embedded systems underlying the explosive growth of interconnected applications.

Over 130 years ago, Dutch linguist and cryptographer Auguste Kerckhoffs stated that a cipher system should not require secrecy and could even fall into enemy hands without causing a problem -- a rule that has come to be known as Kerckhoffs's Principle. Claude Shannon, the father of information theory and electronic communications, reformulated this simply as "The enemy knows the system," now known as Shannon's Maxim.

Commercial embedded systems promise to test these fundamental principles beyond that seen in any other application area. In marked contrast to more conventional secure systems, these systems can be openly acquired by potential attackers, who at their leisure can work to tease out literally every bit of secret information using readily accessible tools.

Semiconductor manufacturers have made great strides in providing strong hardware-based foundations for security. More and more MCUs and specialized processors now include on-chip hardware accelerators for crypto operations, allowing secure real-time communications without loss of performance or increased communications latency. The trend continues in 2015 for inclusion of even more comprehensive hardware support for security. For example, the PIC24F GB2 MCU announced this year by Microchip combines a hardware crypto accelerator with secure on-chip key storage (Figure 1). Although trusted computing and trusted platform modules are beyond the scope of this article, these concepts rely fundamentally on persistent, secure key storage for enabling hardware root-of-trust platforms required for secure boot, trusted software execution, and secure communications in production environments.
Figure 1 The Microchip PIC24F GB2 MCU family combines on-chip crypto acceleration with on-chip secure key storage.

Growing hardware support for security does not necessarily translate into greater assurance of continued security. According to Kerckhoffs and Shannon, companies should assume that the algorithms and, in the present context, the physical circuits used to execute cipher operations are compromised from inception. Basic security policies including layered security and compartmentalization do provide important benefits in complicating the task of would-be attackers. Yet, the notion of security by obscurity has repeatedly been proven inadequate. Current events show that the secrets contained in any system can be exposed by an insider, by a persistent individual, or by organizations with national resources behind them.

Ultimately, the complex formulations of most security policies boil down to a simple underlying notion of Kerckhoffs’s Principle -- that the most important secret in a cipher system is the key used for cryptographic operations. In silicon-based systems, this policy extends to the device itself where differential power analysis (DPA) attacks have been used to reveal keys and other protected secrets accessed during normal circuit operation. When bad actors can so easily acquire and analyze seemingly secure embedded system products, the importance of DPA countermeasures and other underlying circuit protection methods becomes evident.

Inevitably, however, application and system security depend on preserving the secrecy of the all-important cipher key. Indeed, key protection is as old as cipher systems themselves. For protecting national security and military communications, security organizations have long relied on hardware key fill devices (Figure 2) -- portable units containing encryption keys and protected through physical security.
For an embedded design organization, the industry is redefining the physical fill device through enterprise-level security lifecycle capabilities. Typically offered on a proprietary basis by individual semiconductor manufacturers these services provide key generation and protected storage in a secure environment. For example, NXP provides a trust provisioning service along with its A710x secure MCUs. With this service, NXP delivers the MCU with pre-programmed, die-specific keys and certificates that are generated in a secure, Common-Core certified NXP internal environment and stored securely in hardware security modules.

This past year, Rambus' Cryptography Research division announced a solution built around its CryptoManager (CM) Security Engine IP. The new offering, called the CM Infrastructure, places a secure appliance in the local manufacturing plant and provides a central host that serves as root authority (Figure 3). In operation, the local appliance communicates with the host to facilitate key generation and secure storage within the manufacturing facility. During device production, the local appliance securely fills keys in the security engine IP built into a customer device. In turn, the security engine block serves as a hardware root of trust for secure operations within the end product.

Beyond this update to the traditional key fill device, manufacturers are recognizing the need for a broader lifecycle approach to security, where the manufacturer and product developer implement security features that span the entire product lifecycle. In fact, security concerns are fueling a cross-pollination of traditional security and industrial sectors as seen in the agreement announced this past spring between Siemens Industry Sector and Intel’s McAfee unit. Despite the well-publicized penetration of Siemens SCADA systems by Stuxnet, Siemens has been on the forefront of industrial
security -- further demonstrating that even the most carefully woven security blanket can be penetrated by determined sideways attacks.

Also watching:

- **MCU segmentation**: In the early days of the microprocessor industry, the rise of RISC architectures seemed to paradoxically indicate an end to differentiation of a system's base processor. After all, the compiler could do all the heavy lifting so the core need be only simple and fast. Today, even with ARM's dominance of the processor core market, MCUs differentiation is real and profound as MCU makers target specific application segments with devices designed to provide near drop-in solutions for specific applications.

- **Power management**: In a very real sense, the grand vision of an IoT comprising billions of devices is threatened by the simple battery. Without further reductions in power consumption requirements particularly for wireless MCUs, the notion of non-stop data from embedded IoT devices will be limited by design power budgets versus battery capacity. Semiconductor manufacturers continue to push the envelope in enhancing functionality of MCUs while lowering power directly through improved low-power modes and indirectly through improved processing efficiency.

Read more of EDN and EE Times' Hot Technologies: Looking ahead to 2015:

- [Diamonds are a power IC’s best friend](#)
- [Faceless test instruments see the light](#)
- [Fusion heats up](#)
- [GaN: The dawn of a new era?](#)
- [Mobile payment technology reaching critical mass?](#)
- [Smart light's bright future](#)
- [3D printing: To the space station and beyond](#)
- [ADAS takes greater control in 2015](#)
- [Wearables make hardware the new software](#)
- [Changing world requires risk management focus](#)
- [MEMS mics taking over](#)

Also see:

- [Security platform offers root of trust-core: Secure key distribution infrastructure](#)
- [MCUs gain integrated crypto engine with on chip OTP key storage](#)
- [MCU based network processor forms core of simplified IoT wireless connectivity solution](#)
- [FPGAs said to be industry most secure](#)
- [Security demands hardware improvements](#)
- [Mitigate cyber security hazards in smart grids](#)
- [Should your company build or buy its IoT infrastructure](#)