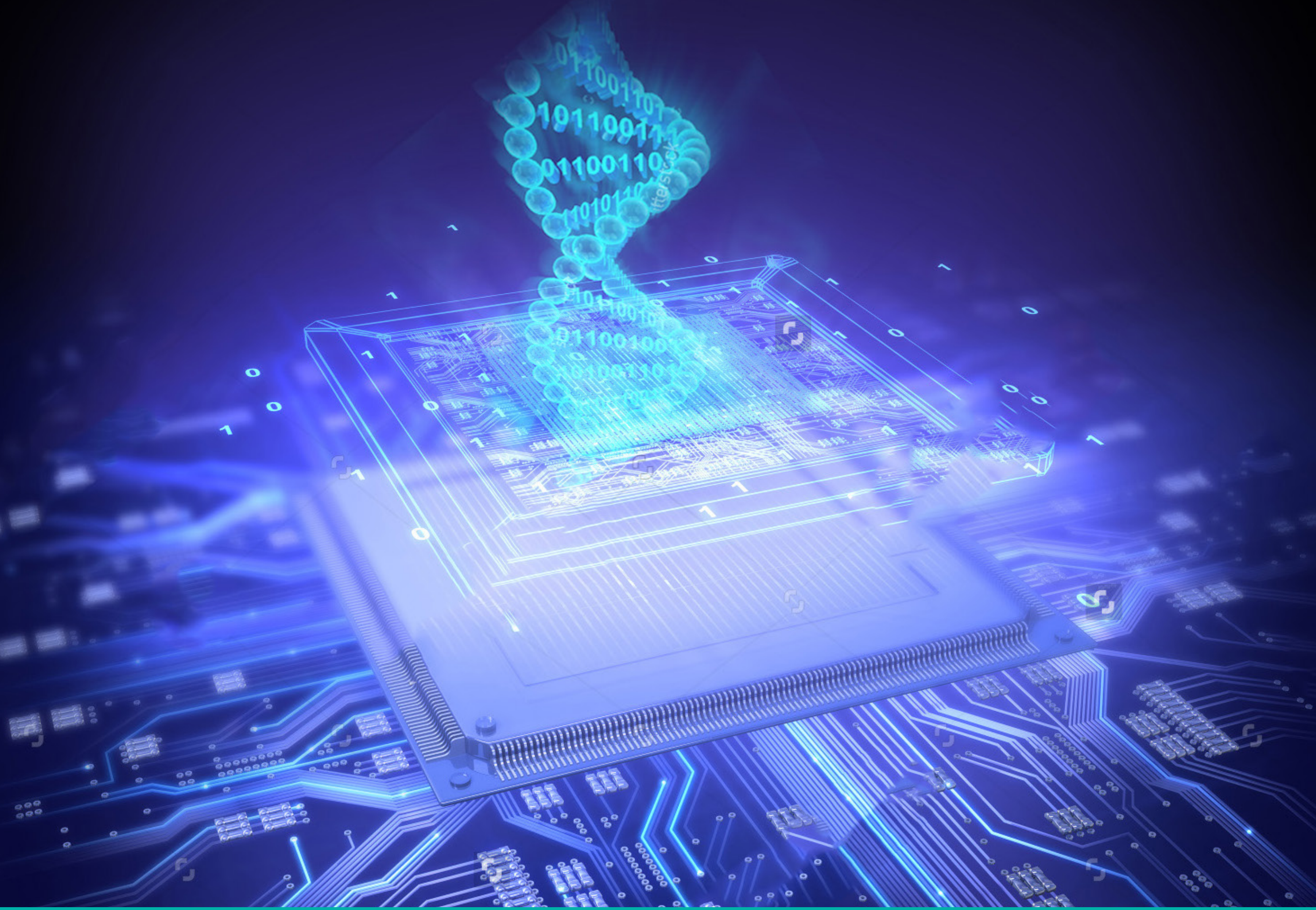

How Unclonable, Turnkey Embedded Security Protects Designs from the Ground Up

By Scott Jones, Managing Director, Embedded Security, Maxim Integrated

November 2017

Abstract

Cybercrime losses rose 24% to more than $1.33 billion in 2016. And these represent only those crimes tracked by the FBI's Internet Crime Complaint Center. News headlines about hacking and other security breaches are a regular occurrence. Yet, design security still remains an afterthought for many product manufacturers. Part of this may stem from the misconception that implementing security is costly in terms of time and resources. This paper dispels these myths and examines the latest in turnkey, cost-effective embedded security that provides strong protection against invasive attacks.

Introduction

Why is Design Security Still Overlooked?

Development of IoT products is outpacing defenses against cyberattacks

Last year, telecommunications giant Telefonica issued a report warning of disastrous consequences as defenses against cybercrime continued to lag behind development of internet of things (IoT) solutions.

"It's not just about the privacy of our own data, or the security of our digital identities. In the next few years our lives will be surrounded by devices connected to the Internet that will digitalize every step we take, convert our daily activities into information, distribute any interaction throughout the network and interact with us according to this information. Never before has what we do in our physical lives been closer to the digital world," noted the company in its report, "Scope, scale and risk like never before: Securing the Internet of Things.[1]"

Yet, security breaches continue unabated. Credit reporting giant Equifax suffered a massive data breach this summer, when hackers gained access to names, Social Security numbers, birthdates, addresses, and some credit card numbers of people in the U.S., along with personal data from people in the U.K. and Canada. This spring, the massive WannaCry ransomeware attack impacted computers in at least 150 countries in Europe, South America, Asia, and North America, hampering hospitals, universities, manufacturers, businesses, and government agencies. The fall of 2016 saw a massive internet outage caused by hacked CCTV video cameras and DVRs, courtesy of a botnet based on the Mirai malware strain. For each of these major, well-publicized incidents, there are many smaller occurrences that should be just as worrisome to consumers and businesses alike. It also goes without saying that as more products and systems become connected, and hackers grow increasingly sophisticated, there are risks that every vertical industry should address. For example, consider these scenarios:

- Industrial: The transition from previously isolated to now fully networked systems exposes equipment to remote attack
- Healthcare: Here, there are privacy issues around sensitive data, data integrity concerns, and the need for authenticated operation of medical equipment/devices
- Banking: Exponential growth of online banking expands the risks since institutions can no longer guarantee identity visually
- Retail: Mobile devices are running open architectures, but because they're acting as financial/payment terminals, they must ensure that transactions and communications are secure
- Communications: End-to-end security is a must to protect against a variety of attacks
- Automotive: Remember back in 2015, when that Jeep was remotely controlled

by white-hat hackers[2]? Hacking of cars, which are quickly becoming computers on wheels, remains a risk.

Neglecting design security is costly in terms of lost revenue, damage to brand reputation, and even personal harm. Patching up systems after a breach occurs is often too little, too late in terms of effectiveness. Truth be told, the earlier in the design cycle you can build in security, the better. Hardware-based security has proven itself to be more effective than its software-based counterpart (Read the white paper, "Why Hardware-Based Design Security is Essential for Every Application," for a comparison of hardware- versus software-based design security.) And fortunately, a hardware-based approach using secure ICs doesn't necessarily require a lot of effort, resources, or time.

The Price of Foregoing Security

While you may be under great pressure to get your product to market quickly while also keeping development costs down, have you carefully considered the cost associated with a breach? As a hypothetical end product in Table 1 shows, foregoing security can actually be costlier in the end.

Hardware-based security provides robustness in part because it is difficult for cybercriminals to alter the physical layer in a design. Additionally, the presence of a physical layer makes it impossible for malware to infiltrate the operating system and penetrate the virtualization layer in a design. By starting at the beginning of your design cycle, you can integrate security into the base level of your design and all of the layers that follow.

Using a secure IC, such as a microcontroller that executes code from an internal, immutable memory, protects against attacks that attempt to breach an electronic device's hardware. The microcontroller's ROM stores the start-up code that is considered to be the "root of trust" because it cannot be modified. This non-modifiable and, therefore, trusted software can be used to verify and authenticate an application software's signature[3]. When a hardware-based "root of trust" approach is implemented from the bottom up, you can close off more potential entry points into your design.

Neglecting design security can lead to lost revenue

Without Security IC	
10 Mu Sales @ $10	$100M
Less 15% counterfeit	**-$15M**
Net Sales	**$85M**
Product Cost, 10Mu @ $3	-$30M
Profit	**$55M**

With Secure Authenticator @$0.50	
10 Mu Sales @ 10$	$100M
Less 0% counterfeit	$0M
Net Sales	**$100M**
Product Cost, 10Mu @ $3.50	-$35M
Profit	**$65M**

Table 1. Loss of assets from counterfeiting ultimately outweighs the cost of implementing security.

Embedded security ICs, such as secure microcontrollers and secure authenticators, provide turnkey solutions that protect entire systems, from each sensor node to the cloud. Not all security ICs are created the same, however. Some secure microcontrollers, for instance, aren't suited for IoT devices or endpoints because of their cost, power consumption, or the complex firmware development required. Then there are cryptographic controllers that implement full security for embedded, connected products without any firmware development. One such example is Maxim's MAXQ1061 DeepCover® device. The coprocessor can be designed in from the beginning or integrated into an existing design to guarantee confidentiality, authenticity, and device integrity.

Secure authenticators are cost-effective IP protection

As for secure authenticators, devices should offer a core set of fixed-function crypto operations, secure key storage, and other related functions that are suited for IoT and endpoint security. With these capabilities, secure authenticators can be a cost-effective means to protect IP, prevent cloning, and authenticate peripherals, IoT devices, and endpoints.

What else should you look for when evaluating embedded security technology? Seek secure microcontrollers with built-in cryptographic engines and secure boot loader that can guard against threats such as cryptanalysis intrusions, physical tampering, and reverse engineering. Design SHIFT, a Menlo Park, California-based digital security and consumer product engineering company, required such features for its ORWL secure desktop PC. When the company was designing ORWL, which requires two factors of authentication and guards against physical attacks, it needed strong root-of-trust security. Design SHIFT found its solution in the MAX32550 DeepCover ARM® Cortex®-M3 secure microcontroller.

"Lots of software guys say, once you lose control of the hardware, you're done," said Olivier Boireau, Design SHIFT's CEO. "Establishing a root of trust provides the reassurance of strong protection."

Strengthening Protection Via Physically Unclonable Function Technology

A more advanced level of cryptography that we're starting to see in security ICs is the physically unclonable function (PUF). PUF is a function that is derived from the complex and variable physical/electrical properties of IC devices. Because PUF is dependent on random physical factors (unpredictable and uncontrollable) that are introduced during manufacturing, it is virtually impossible to duplicate or clone[4]. PUF technology natively generates a digital fingerprint for its associated IC, which can be used as a unique key/secret to support algorithms providing authentication, identification, anti-counterfeiting, hardware-software binding, and encryption/decryption.

Maxim's PUF circuit relies on the naturally occurring random analog characteristics of fundamental MOSFET devices to produce cryptographic keys; the solution is called ChipDNA™ technology. A patented approach ensures that the unique binary value generated by each PUF circuit is guaranteed to be repeatable over temperature and voltage and also as the device ages. The high level of security comes from the fact that the unique binary value is not actually stored anywhere on the chip in non-volatile memory. It is generated when needed by the PUF circuit, then disappears. Thus, unlike previous secure devices, which can suffer from invasive physical attacks on non-volatile memory in an attempt to discover secret key(s), a PUF-based device is not susceptible to this type of attack because you cannot steal what is not there. Furthermore, if a PUF-based device is subjected to an invasive physical attack, the attack itself can cause the electrical characteristics of the PUF circuit to change, further impeding this type of attack. ChipDNA PUF technology has demonstrated excellent reliability over process, voltage, temperature, and aging. Additionally, PUF output evaluation to the NIST[5]-based randomness test suite is successful with pass results. Figure 1 depicts different use cases for ChipDNA PUF technology: internal memory encryption, external memory encryption, and authentication key generation.

First Secure Authenticator with PUF Technology

Maxim's first secure IC featuring ChipDNA PUF technology is its DS28E38 secure authenticator, designed to deliver cost-effective protection against invasive physical attacks. The DS28E38 (Figure 2) provides:

- FIPS186 ECDSA-based challenge/ response authentication
- ChipDNA secured stored data, optional ECDSA-P256 private key source
- 2kb EEPROM array for user memory and public-key certificate
- Decrement-only counter with authenticated read

Root-of-trust can't be modified

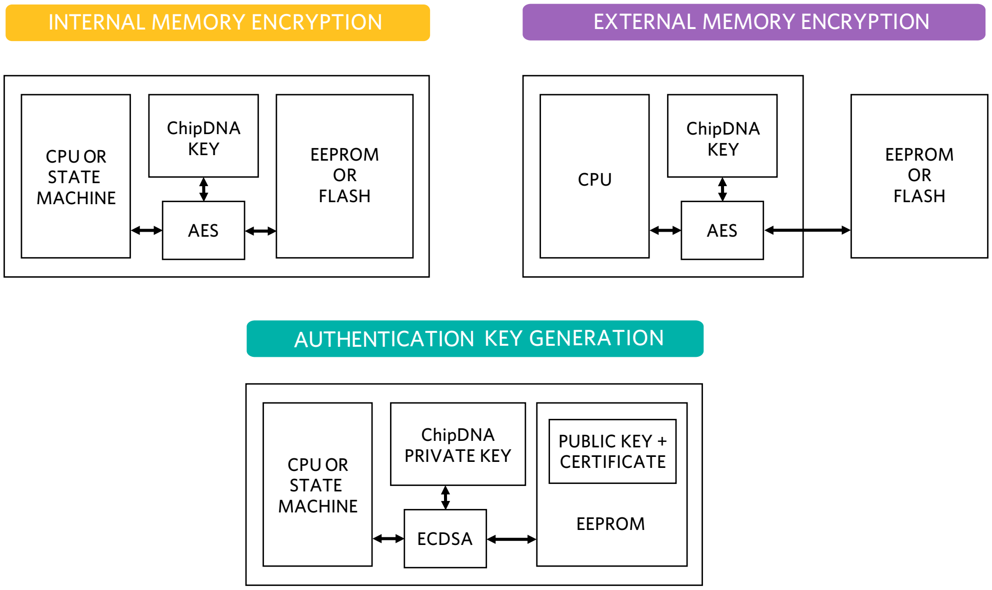

Figure 1: Different use cases for ChipDNA PUF technology.

PUF technology has no key to steal

- Unique factory-programmed read-only serial number (ROM ID)
- Single-contact, 1-Wire® parasitic interface, providing a versatile, rugged, and reliable interconnect method for secure authentication in areas where this was not previously possible.

The DS28E38 is just the first product incorporating ChipDNA PUF technology. Maxim is enhancing its entire embedded security portfolio, both secure authenticators and secure microcontrollers, and will be delivering many new products built with ChipDNA technology in the coming months.

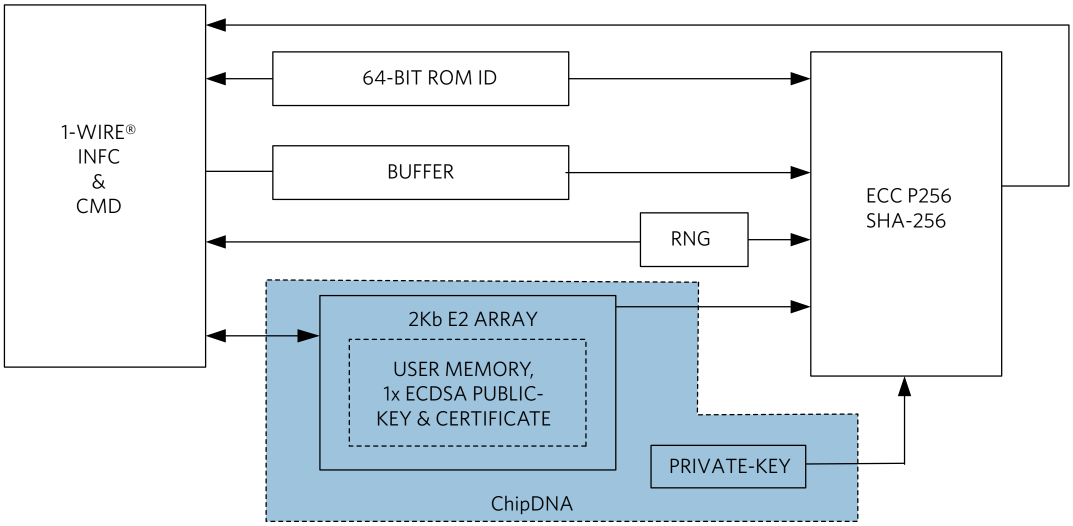

Figure 2: Block diagram of DS28E38 DeepCover secure ECDSA authenticator with ChipDNA PUF protection.

Summary

Today's embedded security ICs provide turnkey technologies to protect your designs from the ground up with layers of advanced security, support for cryptographic algorithms, tampering detection, and many other safeguards. PUF technology, in particular, offers a very strong mechanism to protect against invasive and non-invasive attacks alike. After all, you can't really steal a key that isn't there.

For More Information

Learn more about embedded security solutions that can safeguard your next design from our Embedded Security Selector Guide.

Sources

[1] https://www.telefonica.com/documents/737979/5540857/Telef%C3%B3nica_Security_IoT_Final.pdf/a28293d4-f15a-4f21-8353-317faf892a18

[2] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/

[3] http://www.embedded.com/design/safety-and-security/4438300/Securing-the-IoT--Part-2---Secure-boot-as-root-of-trust-

[4] https://en.wikipedia.org/wiki/Physical_unclonable_function

[5] https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software