Keywords: hardware security, secure authenticator

TUTORIAL 5716

Hardware Security ICs Offer Large Security Returns at a Low Cost

By: Christophe Tremlet, Security Segment Manager
Jul 31, 2013

Abstract: In the face of security vulnerabilities in health and safety applications, governments and industry leaders have focused on security weaknesses in the design and protection of electronic devices. This article explains how using hardware security ICs dramatically reduces the risk of unauthorized access to vital devices, peripherals, and computer systems at a low cost and with minimal impact on designs.

Vulnerabilities to attacks in critical systems are driving growing awareness for the need for improved security methods. Although the industry has relied largely on software-based cybersecurity methods, hardware-based methods are quickly gaining recognition as uniquely capable of delivering strong protection and providing a basis of trust well worth their incremental cost. The emergence of cost-effective silicon solutions enables designers to harden designs—dramatically reducing the risk of unauthorized access to embedded devices, peripherals, and systems, with minimal impact on overall cost.

Take this example:

> *A cardiac patient rests comfortably at home as a state-of-the-art wireless pacemaker delivers a steady stream of pulses to ensure synchronized heart muscle contractions. Unknown to him, a team of opportunistic hackers have stumbled onto his pacemaker system's IP address and unleashed a variety of penetration tools at it. The pacemaker keeps delivering its prescribed signals, protected behind layers of security that defeat each attack, until the hackers give up and continue their scan for easier targets. The patient is never aware of the attempt as he continues to rest peacefully.*

Although this scenario is imaginary, it lies well within the realm of possibility. In fact, recent alerts by the FDA concerning the vulnerability of medical equipment have put a sharp focus on the need for trusted systems able to provide a secure foundation for any connected medical device. Reports of similar weakness in today's electronically controlled automobiles and even wireless-enabled traffic systems have made it clear that critical systems for health and safety are vulnerable to bad actors. Paradoxically, given the potentially sizeable impacts to health and safety associated with a successful cyberattack, the cost of including a reasonable level of trust and security in a design is negligible.

For decades, trusted system protocols—such as computer systems and buildings—have relied on

layered protection of resources designed to limit access only to authorized users, software processes, or other hardware devices. To permit access, the protected resource needs to authenticate, or verify, the identity of the requesting entity.

While authentication methods for access to secure facilities rely on multiple authentication factors (including access cards, access codes, and biometric measurements), authentication methods for access to individual computer systems and devices have lagged. Even today, computer system security relies largely on simple IDs and passwords. Yet, IDs and passwords can be compromised, exposing systems to viruses and more insidious malware able to sit quietly and steal confidential assets over a period of time.

In fact, in an alert to manufacturers, the FDA identified weak password security as a key vulnerability, due to "uncontrolled distribution of passwords, disabled passwords, hard-coded passwords for software intended for privileged device access (e.g., to administrative, technical, and maintenance personnel)."[1]

Indeed, devices touching any aspect of health and safety require implementation of authentication methods that are much stronger than traditional IDs and passwords familiar to computer users—and to computer attackers.

Effective Authentication

A more effective approach for authentication calls for the host system to generate a random challenge. For instance, instead of the typical challenge—"What is your password?"—the challenge might be a string of seemingly random characters. In turn, the requesting entity issues an encoded response that includes a message authentication code (MAC), which is calculated using an algorithm that comprehends not only the requesting entities internal data and secret, but also the specific random challenge received from the host. Then, the host compares the received MAC response with the expected response to verify that it is dealing with a recognized entity (**Figure 1**).

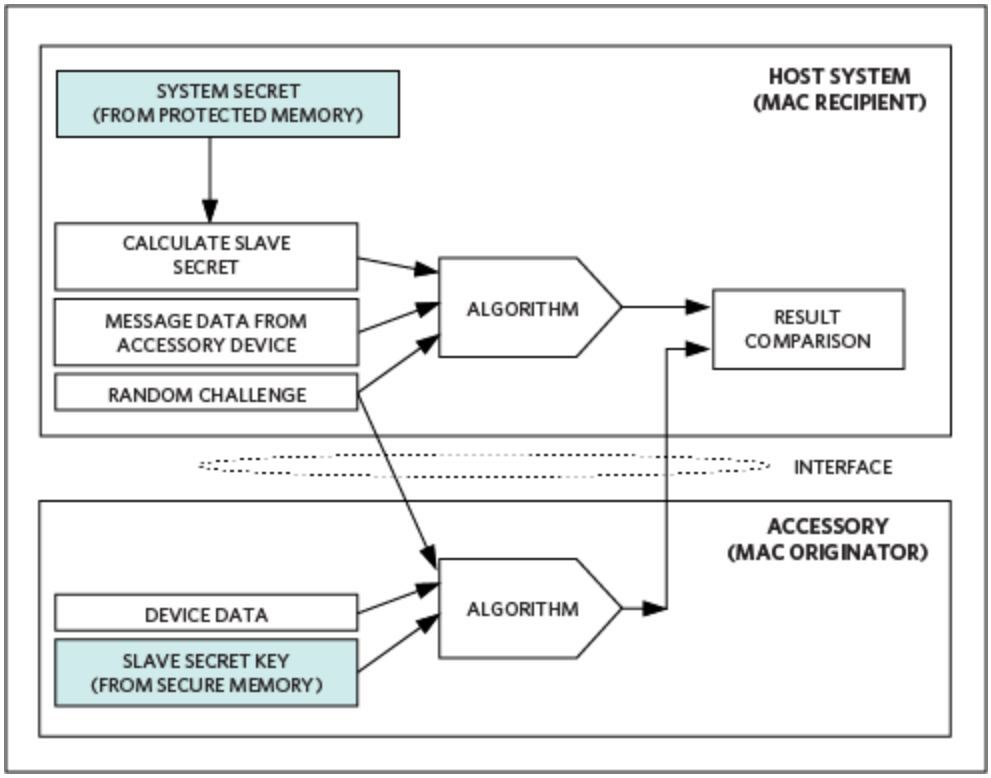

Figure 1. An effective challenge-response authentication method builds a valid response based on a random challenge to verify the identity of an authorized accessory.

With this more robust challenge-response authentication approach, a wireless pacemaker, for example, can confirm that it has received a valid MAC, ensuring that it is communicating with an authorized host before altering its pulse rate. In automobiles, trucks, or heavy machinery, the vehicle's electronic controller unit can respond to apparent emergencies using data streams from trusted embedded devices and peripherals that supply valid MACs.

In the past, companies looking to implement better security measures were forced to choose between robust but expensive hardware such as standalone crypto units or accept the limitations of software-only solutions. A software implementation of a sophisticated challenge-response method may add significant load to a host processor, potentially compromising security responsiveness and overall performance of the host system. Beyond those operational concerns, a software approach remains a weak link in any systems-security architecture. Maintained in normal system memory, secrets remain vulnerable to discovery and modification, while the algorithms themselves run on more general-purpose hardware unable to ensure complete randomness of challenges or even their penetration. The combination potentially exposes the application to attack through a variety of technological and social avenues that continue to be exploited successfully by bad actors.

Specialized ICs that implement security methods offer multiple benefits over software-based security. Specialized crypto chips free host MCUs from the processing load associated with computationally demanding crypto algorithms. Furthermore, these security ICs reduce the points of entry for attackers and provide secure storage for data such as the keys and cryptographic parameters that represent the shared secret. By protecting confidential crypto data and algorithms behind layers of protection, these devices are able to counter all threats more difficult to manage in software-based security.

At a more fundamental level, secure silicon offers the basis for a root of trust that allows engineers to construct higher-level applications with reasonable assurance that the underlying foundation of algorithms and data remains secure. In fact, as discussed later, creating this root of trust in silicon ultimately depends not only on securing the silicon device itself, but also on securing the manufacturing and distribution channel starting at its source.

Secure ICs

Maxim Integrated's DeepCover® secure authenticators leverage unique physical security mechanisms. These authentication devices protect sensitive data under multiple layers of advanced physical security. Attackers face a device using defense-in-depth security that raises the threshold for the cost and timeliness of a successful attack beyond the perceived value of penetration.

Just as important, these hardware security ICs simplify integration. The design simplicity of the 1-Wire® interface used in these low-cost devices facilitates their use in a broad array of applications. In a typical application, engineers need only add a pull-up resistor to connect a spare I/O port of an MCU to a DeepCover authentication device such as the DS28E15 (**Figure 2**).

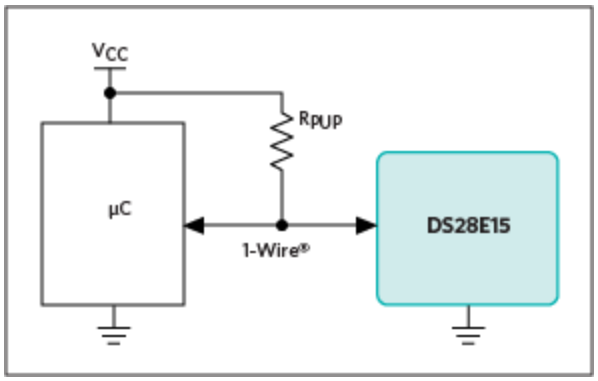

Figure 2. The addition of a pull-up resistor can connect a spare I/O port of an MCU to a DeepCover authentication device.

Consequently, designers can easily implement secure system designs supporting multiple peripherals, each authenticated through a dedicated DeepCover authentication IC. Here, a DS2465 DeepCover IC serves as the 1-Wire master, handling line driving and protocol conversion between the I^2C master and any attached 1-Wire slave authentication ICs.

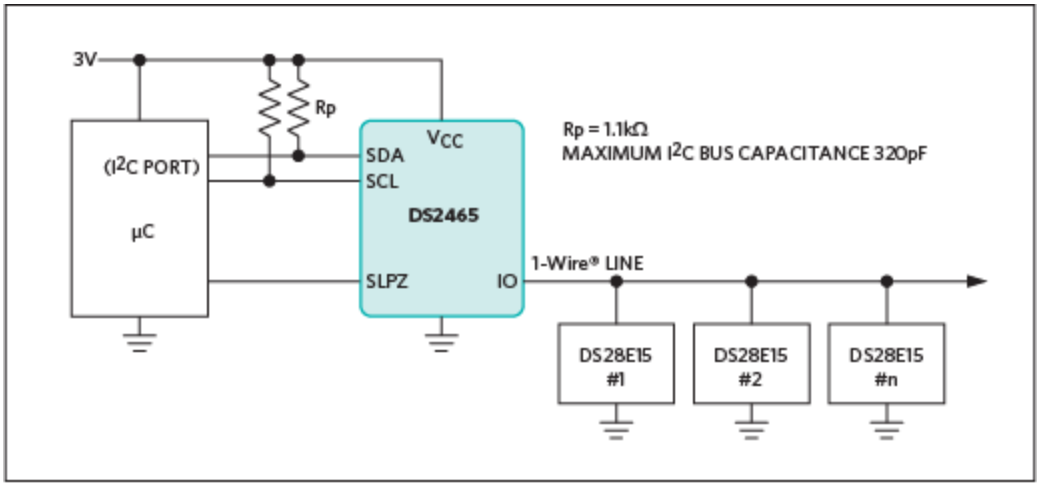

Figure 3. Incorporate a 1-Wire master device such as the DS2465 to handle 1-Wire line driving and protocols on behalf of an MCU.

Within an application, individual members of the DeepCover authentication family support FIPS 180-3 Secure Hash Algorithm SHA-256 and FIPS 186 public-key based Elliptic Curve Digital Signature Algorithm (ECDSA) cryptography. For SHA-256 applications, the DS28E15, DS28E22, and DS28E25 combine a SHA-256 engine and security features with 512-bit, 2Kb, and 4Kb user EEPROM, respectively. For ECDSA designs, the DS28E35 provides 1Kb EEPROM along with its ECDSA engine and associated security features.

Among the security features supported across all members of the DeepCover authentication series, each device combines its user-programmable EEPROM array available for application data with protected memory areas for storing both the read-protected secret associated with the device's supported crypto algorithm and the data parameters. In addition, each device includes a guaranteed unique 64-bit ROM identification number, which serves as input for crypto operations and provides a universally unique serial number for applications.

As mentioned earlier, establishing a root of trust for an IC begins at the factory and through the distribution channel. If a device's internally stored secret were readable or modifiable by unauthorized agents, the security of systems built with that device would be immediately compromised. Besides operational security measures, DeepCover authentication ICs enable secrets to be read-protected from unauthorized access—and write-protected to prevent any modification of the secret. Beyond this protection, the creation of the secret itself can follow recommended security principles of compartmentalization: Rather than creating the complete secret at one location, the secret can be built in stages.

As the device passes through different locations in the supply chain, it can itself generate another portion of the secret. As the authentication IC becomes itself the root of trust for the end product, the same process may apply to the finished product. The complete secret for any individual device would thus remain effectively unknown and beyond the reach of any individual.

In the face of security vulnerabilities in health and safety applications, government and industry leaders have focused on weaknesses in security procedures in the design and protection of vital devices, peripherals, and computer systems. Using dedicated hardware security ICs, companies can build a solid foundation of trust into their products at incremental cost and minimal impact on design. Authentication

ICs such as Maxim's DeepCover embedded security solutions simplify implementation of robust challenge-response authentication methods that form the foundation of more effective application security.

References

1. "FDA Safety Communication: Cybersecurity for Medical Devices and Hospital Networks," June 13, 2013, http://wayback.archive-it.org/7993/20170722144747/https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm356423.htm.

Related Parts		
DS2465	DeepCover Secure Authenticator with SHA-256 Coprocessor and 1-Wire Master Function	Free Samples
DS24L65	DeepCover Secure Authenticator with SHA-256 Coprocessor and 1-Wire Master Function	Free Samples
DS28E15	DeepCover Secure Authenticator with 1-Wire SHA-256 and 512-Bit User EEPROM	Free Samples
DS28E22	DeepCover Secure Authenticator with 1-Wire SHA-256 and 2Kb User EEPROM	Free Samples
DS28E25	DeepCover Secure Authenticator with 1-Wire SHA-256 and 4Kb User EEPROM	Free Samples
DS28E35	DeepCover Secure Authenticator with 1-Wire ECDSA and 1Kb User EEPROM	Free Samples
DS28EL15	DeepCover Secure Authenticator with 1-Wire SHA-256 and 512-Bit User EEPROM	Free Samples
DS28EL22	DeepCover Secure Authenticator with 1-Wire SHA-256 and 2Kb User EEPROM	Free Samples
DS28EL25	DeepCover Secure Authenticator with 1-Wire SHA-256 and 4Kb User EEPROM	Free Samples

More Information
For Technical Support: http://www.maximintegrated.com/support
For Samples: http://www.maximintegrated.com/samples
Other Questions and Comments: http://www.maximintegrated.com/contact

Application Note 5716: http://www.maximintegrated.com/an5716
TUTORIAL 5716, AN5716, AN 5716, APP5716, Appnote5716, Appnote 5716