Solution Brief

Infineon Origa™

Original Product Authentication Solution
SLE95050F1

Introduction

The counterfeiting or cloning of devices and peripherals is a major concern for OEMs. Since most manufacturing is outsourced to offshore Contract Manufacturers (CMs) - and in some cases multiple CMs - it has become almost impossible to protect IP and prevent the unauthorized production of similar products and peripherals. Legitimate companies are not only suffering direct revenue losses, but are also losing brand reputation and image reliability from damaged products as a result of using cloned peripherals, - in some cases even incurring high liability costs.

Many new products are subsidized when introduced in the market; the intended business model is for the sustained after-market sale of accessories and add-ons to recover the initial investment. Some examples of such products are accessories for game consoles, accessories for mobile devices, and printer cartridges. Cloning poses a serious threat to this business model. In some cases, unauthorized accessories can even pose a hazard risk to the end user, thus exposing the OEM to hefty liability costs and damage to the brand reputation. Tamper- and counterfeit-resistant peripherals will not only help OEMs from an economical, reliability, image, and liability perspective, but will also help consumers by ensuring the integrity of the entire system - thus providing the intended user experience and peace of mind to both parties.

Challenges

There are many solutions attempting to address anti-cloning issues; while in many cases some degree of success is achieved, it is often short lived. Patents, custom connectors, and proprietary hardware/software solutions are used to thwart attackers, cloners, and hackers with variable success rates. There is always a trade-off between the cost of protection vs. the value of what is being protected. It is always a challenge to make both the platform and accessory tamper-resistant. Additionally, any potential solution must carefully balance production cost and efforts against the level of difficulty of cloning the peripherals. Any acceptable solution must maintain a balance between adequate security and cost. A successful anti-cloning solution must answer the following questions:

1. Is the host system immune to attack?
2. Is the peripheral immune to attack?
3. Is there a chance to break one and use the information to hack all the systems?
4. Is the security infrastructure programmable with after-market parts?
5. How can one prevent the reuse of expired parts/accessories (cartridge, battery, etc)?
6. Is the solution cost-effective and easy to implement?

In many cases, a software-to-hardware authentication solution is preferred for both manufacturing cost and ease of implementation. In this type of solution, the authentication hardware is located in the accessory and the software resides in Host system. In some cases, OEMs want to protect their software IP by allowing it to run only on original peripherals or add-ons.

Never stop thinking

In this scenario, the shared secret scheme or symmetric solution (in which the Host and peripheral share the same secret) falls short due to the fact that if the Host shared secret is exposed, then original devices can easily be replicated and clones are guaranteed to work with all Host systems.

There are many classes of after-market parts and accessories which are built to be compatible to OEM specification and standards (Notebook AC adapters, batteries, etc.): among these, there are clone devices which are an exact replica of original OEM products, and there are legitimate accessories manufactured by OEM authorized third parties. Now comes the big question, how can a system identify between authorized and unauthorized parts? If the security hardware in the peripheral and/or Host can be personalized at manufacturing, what prevents a cloning manufacturer from purchasing such security hardware and making extra replica parts for more profit?

Origa™ – Original Product Authentication Solution

Infineon is the leader in providing security solutions for many applications such as the US e-passport, Trusted Platform Module (TPM) for PCs, and payment and chip card solutions. Infineon recently added Origa™ to its product portfolio to address anti-cloning for cost sensitive applications.

The Solution

Origa™ is the world's first asymmetric authentication chip featuring elliptic curve cryptography (ECC) and an integrated temperature monitoring sensor. It brings Infineon's market leading security expertise and knowledge to the accessory authentication market. It also incorporates a lifespan indicator (decrease-only counter), user non-volatile memory, and unique serial ID for each device. Personalization (insertion of secret key into the device) is performed at Infineon's secure (EAL5+ certified) production facilities. Origa™ also has some built-in hardware protections to safeguard the protected contents within. Origa™ interfaces with the Host via a single wire protocol (Single Wire Interface (SWI) is Infineon proprietary) which can be also used to power the chip. This simplifies the Host-to-peripheral connection scheme. For details on the features and applications, please refer to the datasheet and other documents on Origa™. Host software reference code is provided by Infineon to ease development efforts and decrease time to market. Now let's take a look at how Origa™ features address most of the challenges in implementing a robust authentication solution.

1. Is the Host system immune to attacks?

There are different types of Host-side software implementation. If the code is implemented in a controller firmware or in BIOS (pre-boot phase), the attacks could come from someone who has physical access to the system. If the code is implemented in a Post OS phase, then attacks could come from remote entities. Attacks to Host systems are aimed at retrieving the secret which would allow counterfeiters to build clones. In the case of Origa™ enabled systems, Host code and libraries only contain public information; the attacker cannot gain any knowledge of the private secret held within Origa™'s protected boundary. An attack on the Host - in order to find the secret key to enable cloning – is therefore futile. From this perspective, the Host system is immune to attacks.

2. Is the peripheral immune to attacks?

Unless anti-cloning solutions incorporate some level of protection, reverse engineering would reveal the secret recipe necessary for cloning. Origa™ incorporates physical security to protect its secret. Due to ECC asymmetric protocol, bus snooping will not reveal any secrets; its implementation also includes protection against replay, side-channel and power attacks. Hence, ORIGA™-based solutions are relatively immune to attacks, especially when it comes to large scale commercial cloning.

3. Is there a chance to break one and use the information to hack all the systems?

Since the Host only contains public parameters and Origa™ contains the secret key and parameters, it is not possible to extract private information by manipulating the Host. There is no possibility of the "break-once-and-publish-everywhere" scenario seen with symmetric algorithms. As the market leader in security ICs, Infineon can leverage its manufacturing and personalization facilities for high security products like banking, government ID and Pay TV for an efficient authentication device like ORIGA™. (ORIGA™ uses the same EAL5+ certified security management system in the production facilities). Origa™ personalization at Infineon's secure facility also prevents secret leakage from accessory manufacturing sites.

4. Is the security infrastructure programmable with after-market parts?

Origa™ personalization is possible for each particular customer or even for each SKU (stock keeping unit) or sub group of products for the same customer. Those dedicated SKUs will be supplied only to customer-designated manufacturing sites and will not be available for purchase by any other entities. No Origa™ product will be available without personalization in the general market for personalization at manufacturing sites. ORIGA™ is always personalized in the Infineon secure personalization facility.

This secure personalization process serves several purposes:

- It is not possible to buy blank Origa™ and personalize them for cloning.

- It prevents secret leakage from manufacturing or ODM sites.
- It eases the manufacturing process (eliminating key or secret injection and key management logistics) by saving cost and reducing production time.

5. How can one prevent the reuse of expired parts/accessories (cartridge, battery, etc)?

The lifespan indicator can be used to permanently retire any part or accessory. A combination of unique ID, NVM data, and lifespan indicator can be used for this purpose as well.

6. Is it cost effective and easy to implement?

As the leader of Security Solutions, Infineon understands the fine balance between cost, degree of security, and ease of implementation. Origa™ is architected and designed with all these factors in mind; it can meet stringent security requirements while allowing easy implementation with reasonable cost structure. Infineon provides the code library package which also contains the ECC library, simplifying the implementation process and saving time. The personalization process also relieves the OEM and CM of key management logistics, key injection steps, and secret leakage issues which helps from a cost and implementation perspective.

Conclusion:

It is a well understood fact that certain applications require an efficient level of security while being cost sensitive. For example, printer cartridge manufacturers would like to protect their revenue stream, and cell phone manufacturers would like to protect their device reliability and brand via anti-cloning techniques; however, both applications are cost sensitive in nature. Origa™ addresses these requirements for peripheral authentication and yet remains an economically justifiable and easy to implement solution.

Published by:

Infineon Technologies North America
640 N. McCarthy Blvd
Milpitas, CA 95035
www.infineon.com/ORIGA
E-Mail: ORIGA@infineon.com