How Secure Fuel Gauges Can Prevent Battery Counterfeiting

By Perry Tsao, Executive Director, Mobile Solutions Business Unit, Maxim Integrated

March 2018

maxim integrated™

Abstract

While cloned battery packs might seem like a cost-effective option, they typically aren't made with the protective and safety features that their authentic counterparts have. As a result, these clones could cause damage or personal harm. For battery manufacturers and OEMs, counterfeits represent lost revenue. This paper examines different approaches for preventing battery counterfeiting and takes a look at how battery fuel gauges with built-in security can offer a strong level of protection.

Introduction

What Makes Counterfeit Batteries So Dangerous?

Counterfeit batteries mean lost revenue and, potentially, brand reputation harm and liability issues

In early 2016 in Nashville, Tennessee, a $1 million home was destroyed by a fire that was started when a hoverboard's battery overheated. A lawsuit led by the homeowners alleges that the hoverboard was a counterfeit, rather than a known product containing a brand-name battery as advertised. Many other cases of hoverboard-related fires followed. That year, the U.S. Consumer Product Safety Commission recalled more than 500,000 hoverboards from 10 companies, noting that poorly designed lithium-ion batteries can overheat and potentially catch fire or explode.

In genuine lithium-ion battery packs, you'll typically find battery cells with safety features; protection circuits that guard against overcharging, overdischarging, and overcurrent; and protective devices that isolate any overcurrent. Counterfeit battery packs look just like the real thing and are typically cheaper than their authentic counterparts; however, they often lack safety components or protective devices. What's more, many of them have problems like substandard or unqualified cells, mismatched components on circuit boards, poor connector design, poor insulation, and bad welds or solder joints.

While their risks can potentially hurt consumers, gray market batteries are also damaging for original equipment manufacturers (OEMs). For OEMs, counterfeiting means lost revenue and, potentially, brand reputation harm and liability issues.

With consumer electronics being the second most pirated items in the U.S., it's really not surprising that cloned batteries have become a big problem. In fiscal year 2017, the U.S. Customs and Border Protection (CBP) seized and destroyed almost 32,000 shipments of counterfeit goods, which consisted of more than just counterfeit batteries. But, as CBP noted in a November 2017 blog post: "Counterfeiters focus on trends to make fake versions of popular products, such as smartphones or makeup. Maybe you remember the hover board craze from late 2015 and early 2016. Many of those products contained counterfeit batteries, which ended up sparking fires and causing significant safety concerns."

According to a Scout CMS blog post, smartphone batteries in particular are attractive for consumers who want a good deal, "but the bad part of the deal is that smartphone batteries involve complicated engineering that can malfunction—even without being hacked."

In fact, the problem of counterfeit batteries extends beyond consumer applications into medical and industrial applications that need to operate reliably even in harsh conditions.

What can you do to protect your customers and your company?

A Look at Various Battery Authentication Approaches

As with any product, authentication ensures that a product is genuine and guards against counterfeiting. To be effective, the battery should be authenticated before a system is allowed to charge or even function with the battery. For example, an authentication routine could be run when external power is supplied to charge the battery. Or, a system being powered by the battery can be set up to refuse power from the battery if authentication fails.

There are various methods for authenticating batteries. The most basic approach is to place a resistor in the battery pack to identify battery type. Adding another level of security, battery designers can include a memory chip in the pack with information such as cell voltage, manufacturing date, and the battery ID. Another once-popular method for battery replacements is form factor authentication. Based on this approach, the battery casing and connectors are molded to fit the application. However, third-parties can easily produce the exact physical replicas of both to create their clones.

An electronic challenge-and-response methodology can provide stronger protection if implemented properly. The most basic implementation of this form of electronic authentication is via an unchanging bit-stream challenge that seeks a simple bit-stream response. This method can work reasonably well if a large number of unique challenge-response pairs are distributed within the population of the device using this system. In this system, the host system doesn't need to keep any secret and worry about keeping it secure.

Unfortunately, a hacker can defeat this approach fairly easily by monitoring the bit-stream and copying the bit-stream response.

Fortunately, there are battery fuel gauge ICs that implement an advanced challenge-response scheme that is far more secure. Maxim fuel gauge ICs, for example, implement a method that is secured by a cryptographic SHA-256 hash algorithm. They also implement advanced IC design features that make stealing the secret authentication codes impractical for even determined hackers. Not only does this approach provide valuable battery state-of-charge (SOC) data, but it also presents a relatively easy and cost-effective way to prevent cloning.

Choosing the Right Secure Fuel Gauge IC

Battery fuel gauges with secure authentication utilize unique keys that render the theft of a secret from a single IC to be useless. ICs that use multi-step secret key generation offer a robust approach to prevent secrets from leaking from manufacturing sites. Multi-step secret key generation works like this:

- First, a secure hashing method is used to create Secret1
- Next, the same hashing algorithm and the chip's unique ROM_ID are used to create Secret2
- Secret1 is overwritten, while Secret2 is stored in the IC and is different for every IC

Figure 1 depicts the process of unique secret key generation.

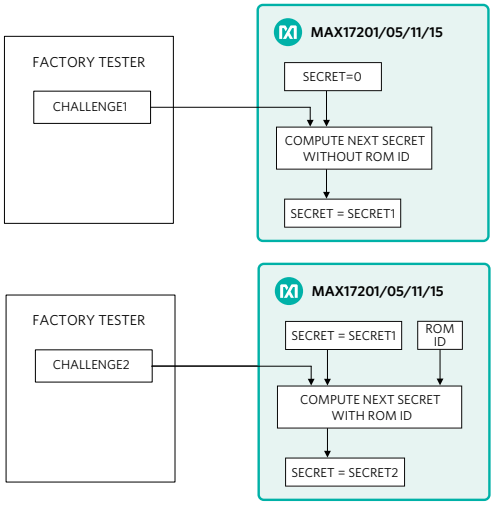

Figure 1. Unique secret key generation using the MAX17201/MAX17205/MAX17211/MAX17215 fuel gauge ICs with built-in secure authentication

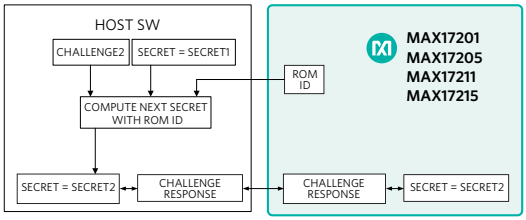

Figure 2. Authenticating the battery in the host software, using the MAX17201/MAX17205/ MAX17211/MAX17215 fuel gauge ICs with built-in secure authentication

Battery pack manufacturers do not need to know Secret1 or Secret2, which minimizes the risk of the secret keys being leaked. The two separate challenges used are secured at the factory. As long as at least one of the multiple steps remains protected, the secret is safe. Based on these factors, a secret created via this challenge-and-response approach is safer than one that is written directly into the IC. To further safeguard against theft of the secret key, the IC provides immunity to optical, electrical, timing, and power analysis, as well as to physical inspection via deprocessing.

Figure 2 depicts the process to authenticate the battery in the host software. The host software uses Challenge2, Secret1, and the ROM_ID to generate Secret2. The host software then conducts a challenge-response method to authenticate that the fuel gauge knows Secret2. The host software must securely store both Challenge2 and Secret1.

SHA-256 Authentication and Unique, 160-Bit Secret Keys

Maxim's **MAX17201**, **MAX17205**, **MAX17211**, and **MAX17215** ModelGauge™ m5 fuel gauge ICs are an example of chips that meet the authentication criteria discussed. These FIPS 180-4-compliant ICs with SHA-256 authentication have 160-bit secret keys that are generated uniquely for each battery at the factory using multi-step key generation. The secret key cannot be physically read from the fuel gauge and its verification can be completed only via the challenge response.

As a counter-measure against deprocessing, the ICs have optical inspection immunity. Ones and zeroes stored in the nonvolatile memory aren't physically distinguishable. The fuel gauge ICs have immunity against electrical inspection such as microprobes and e-beam probes, as the key isn't stored plainly in the nonvolatile memory. Their physical design uses the top metal layer for routing power, ground, and other signals without critical information. Critical signals are covered in electrically biased metal areas. If someone tries to remove the top metal layer, this action would render the chip inoperable. Neither micro probing nor voltage contrast can reveal the secret with all of the signal layers intact. The ICs also have timing analysis and power analysis immunity (the timing of the SHA calculation is independent of the key, and power consumption during internal key access is independent of the value of the key). In addition, the timer value is stored in life logging registers (registers that cannot be altered later), providing a countermeasure against cloning.

Unfortunately, there are other fuel gauges on the market with less secure authentication schemes and physical design. In some cases, it appears that the secret keys have been stolen and counterfeit batteries are readily available for sale in the market. Selecting a fuel gauge IC with strong security features is essential to stopping counterfeiting.

In addition, the MAX17201, MAX17205, MAX17211, and MAX17215 ICs feature the ModelGauge m5 EZ fuel gauging algorithm, and they deliver high-accuracy SOC estimation without the need for battery characterization. The ModelGauge m5 EZ algorithm brings together the short-term accuracy and linearity of a coulomb counter with the long-term stability of a voltage-based fuel gauge plus temperature compensation. The ICs automatically compensate for cell aging, temperature, and discharge rate, providing accurate battery SOC in mA-hr or percentage over a wide range of operating conditions. The design of these ICs taps into Maxim's more than 20 years of experience in security, including in areas such as cryptographic algorithms, IC-level physical protection, and security-oriented manufacturing flow.

ModelGauge m5 fuel gauge ICs feature SHA-256 authentication

Summary

By integrating a secure battery fuel gauge IC into your design, you can protect your battery packs cost-effectively and with relative ease. A fuel gauge IC can provide an accurate measure of the battery's SOC and also guard against cloning, hacking, and other illicit acts.

Learn More

Find out more about ModelGauge fuel gauge technology.

Learn more

For more information, visit:
www.maximintegrated.com