

Product group : Digital ICs

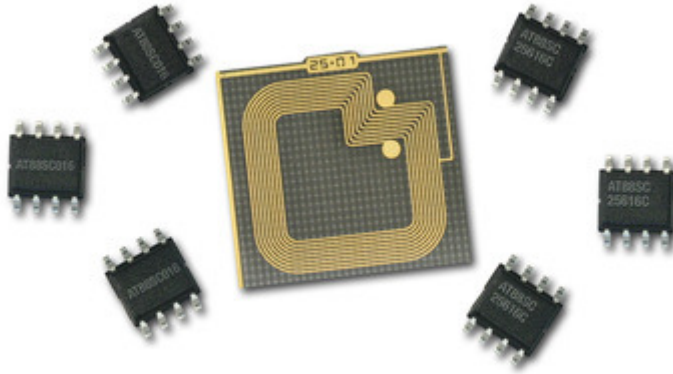
Product Sub-group : Encryption ICs

Reference:

31255

Product Counterfeiting - Why It Is so Difficult to Prevent

A counterfeit product is defined as a product that has been manufactured, without authorisation, by someone other than the bona fide product vendor or manufacturer. The cost of counterfeiting is far more than the billions of dollars worth of phony products seized last year. Fake goods can cause customer-service problems and damage to a company's reputation. And if they are electrical appliances, the consequences of forgery could be life-threatening. EPN, 15/06/2008



In many cases, product counterfeiting is fairly easy to do. It requires two things: firstly a fake product, and secondly a copy of the real label, logo or packaging used to identify it. In many cases, anyone with a fairly standard scanner and a printer can get the job done. The rest of the time, it is more difficult to do and requires the cracking of encryption algorithms or the dismantling and microscopic analysis of an IC. If enough money is involved, a dedicated counterfeiter will usually find a way to create and market the fakes.

Electronic methods of defeating counterfeiters

The entertainment, drug and fashion industries, in particular, have spent decades attempting to thwart product counterfeiters. Solutions include simple labeling with logos or barcodes to software algorithms used in digital-rights management to embedding integrated circuits in the product or its packaging. However, most attempts to prevent product counterfeiting fail.

The majority of counter-piracy solutions are software-based. The algorithms, encryption keys and passwords are implemented in software that is stored in some kind of memory. There are basically three ways to crack software-based security: gaining access to the actual encryption key, changing the signature of that key or eliminating the need for a key. The key is usually stored somewhere in the end-user equipment, probably on a hard-disk drive or in a memory chip inside this device. There are three ways of getting this key: algorithmic attacks, systematic attacks and physically dismantling the device itself. Algorithmic attacks involve the collection of copious amounts of data prior to, during, and after algorithmic processing. Sophisticated statistical analysis or brute force trial-and-error can be used to tease the cryptographic key from within the data.

But there is also hardware security: while many industries use software to try to prevent access to digital content, others - such as those who manufacture drugs or fashion items - have begun using integrated circuits as a kind of electronic label. The simplest form of electronic labelling is to embed a standard serial EEPROM inside the product or package. The EEPROM can have a standard two-wire interface or an RF interface, such as those on RFID tags (Figure 1).

Figure 1: An example of an EEPROM label.

The EEPROM serves as memory to hold digital information. This information can be the digital encoding of the actual product name and specific identifying details like version numbers. This information can also be just a record number that references the actual product information in a database somewhere, just like conventional barcodes. The memory capacities of such labels typically range from a few bytes up to 128bytes. In volume, they cost as little as fractions of pennies.

Other than the fact that the label information is stored in an integrated circuit, the security of EEPROMs is very low. Instead of using a copier, the product counterfeiter can use a sub-\$100 EEPROM reader to read the information from an existing EEPROM label and then simply copy it into blank serial EEPROMs that it can use in the packaging of the bogus product.

EEPROMs with encrypted IDs

To overcome the inherent lack of security in EEPROMs, some vendors offer designers the ability to assign unique serial numbers to each EEPROM-based label, which are then encrypted using strong algorithms. The host equipment combines the EEPROM's unique serial number with a cryptographic key that is known only to the EEPROM and then applies a very strong hash algorithm - like SHA-1 or AES-CC - to the combined information to create a large number with as many as 20bytes, called a digest, which it stores on the EEPROM.

Hashing algorithms are very strong, and the resulting numbers are virtually un-crackable. This approach is considered by many product vendors, distributors and retailers to be fool-proof. Unfortunately that is not the case: it is not necessary to defeat the encryption algorithm or crack the keys to create a fake electronic label. As with the simple EEPROM label, creating valid but fake labels only requires a low-cost EEPROM reader that can copy the information from the EEPROM and re-write it on blank ones. The product counterfeiter does not need to decode the information on the label: he or she only needs to copy it.

Password-protected EEPROMs

The only way to prevent the authenticating product information from being copied from an EEPROM-based label is to prevent access to it. A few vendors have addressed this issue by requiring passwords and/or keys to access the data on the EEPROM. Passwords, which may be embedded in the silicon, help to limit access to the identifying product data that could be used to create fake electronic labels. Although password-protected EEPROMs offer much improved security at a relatively low price, they have a drawback that makes them unsuitable for high-value or safety-sensitive products such as pharmaceuticals. Encrypted or not, the passwords are still stored in the EEPROM itself. In many cases, the EEPROM contents can be dumped using a standard, low-cost EEPROM reader. There are real-life cases in which the passwords, keys and administrative pins have been read directly from the device with no special effort at all. This information can be used to create clones of the security device itself, which can be affixed to fake products. Cloning can be accomplished even if the password is embedded in the silicon.

Although these more elaborate electronic labels provide much higher security than paper labels, bar codes or unprotected electronic devices, they are really software-based solutions, with the encryption algorithms, keys and passwords implemented in software and stored on the device.

True hardware-based cryptographic security

Some vendors have developed a new type of low-cost cryptographic memory that offers true hardware-based security for electronic labels. Cryptographic memories have a hardware-based cryptographic engine embedded in the silicon, plus multiple sets of separate non-readable, authentication and session encryption keys, each up to 64bits and all stored in up to 2kbits of configuration memory.

The security in a cryptographic memory is not based on identity *per se*, as defined by passwords and keys, encrypted or otherwise. It is based on authenticity, which is determined by hardware inside the device and hardware-stored keys that generate unique cryptograms. The cryptograms are used by the device to identify an authentic host and by the host reader to identify the device as an authentic label. The various keys used to create the cryptograms are truly secret because they are set in hardware by the host device. Once set, fuses in the cryptographic memory are blown, rendering the keys unreadable - even by the host. The authenticating information on the cryptographic memory never sees the light of day and cannot, therefore, be copied or intercepted, even by the silicon manufacturer. Unlike the simple passwords in software-based technology, the information used to authenticate cryptographic memories is not just encrypted, it changes with every transaction.

The majority of labeling techniques, from barcodes to EEPROMs to password-protected RFID tags, cannot effectively prevent product cloning as they rely on software-based security techniques that can be all too easily read directly from the device or derived by observing and analysing secure transactions between host readers and devices. The only reliable way to protect product authenticity is to shield it from prying eyes. This means locking it in the hardware of the labeling device and never ever transmitting it during transactions. Cryptographic memories are the only electronic labels that create unique signatures for each and every transaction, based on information that is never ever transmitted or allowed to be accessed in any way. The signature can be verified by an authentic host, but the authentication keys on which the signature is based can never be read. As a result, cryptographic-memory-based product labels are virtually impossible to clone or copy.

By Eustace Asanghanwa, Atmel

Atmel Corp
2325 Orchard Parkway
95131 San Jose - USA
tel: +1 408 436 4205
fax: +1 408 487 2600

Company website