Keywords: Secure controller, secure memory, secure SRAM Controllers, Battery Backed Controllers, FIPS, FIPS 140, common criteria, ATM, POS, Software Defined Radio, SDR, Financial terminal, Encryption Key Protection, SRAM Erasure, Data Protection,

APPLICATION NOTE 3976

Embedded Security Going Forward

Jan 30, 2007

Abstract: Equipment manufacturers and designers are facing many new design challenges due to the continuing need for increased data security in many of today's electronic systems. At the heart of the problem is the need to either implement security and antitamper countermeasures into a new application that never before required such mechanisms, or to avoid the introduction of new design variables into proven existing security circuitry. This is compounded with the emergence of new security standards and the the ever-increasing demands the certification bodies require. The challenges of maintaining size and cost competitiveness further complicate this critical design requirement. In order to meet these challenges, Maxim has introduced a family of innovative devices designed to specifically address new and emerging security standards in a controlled and layered approach. The following describes how these new devices allow legacy designs to be enhanced with additional security, while minimizing the costs and risks of designing entirely new embedded security platforms.

This article was also featured in Maxim's Engineering Journal, vol. 59 (PDF, 497kB).

With the rapidly growing concerns of security in nearly every aspect of electronic system design, manufacturers and circuit designers will soon face challenges that never before existed. In the past, security within electronic equipment was something only faced by a limited and very selective audience consisting mostly of software-related technologies or specialized hardware used in financial, military, and access-control markets. This is all about to change as designers will soon be given a host of new standards to meet, certifications to obtain, and technical knowledge to learn that will seem foreign to many seasoned designers of embedded electronic systems. Understanding this technological trend, as well as its design and manufacturing cost ramifications, is of growing importance to equipment manufacturers of embedded systems.

Because ensuring software/firmware integrity is an extremely complex issue, the burden is placed upon hardware to maintain security and not become the weakest link in a complex security implementation (see *Appendix 1—Classification Taxonomy*). With the formation of new standards bodies like the Trusted Computing Group™, as well as various digital rights management (DRM) proponents, the issue of security is rapidly affecting a broad range of devices, including consumer, media, industrial, medical, automotive, and telecommunication equipment. Of course, this issue also includes governmental or homeland security system upgrades and the increased proliferation of electronic banking and e-commerce applications.

However, for any security solution to be effective, physical tamper protection and the methods to achieve it must be addressed. Even the most sophisticated secure microprocessors, FPGAs, smart cards, and other security components still remain vulnerable to certain attack scenarios. This vulnerability leads to the requirement of maintaining a suitable portion of active circuitry, which remains "alive" during system downtime to sense a potential attempt to extract or steal sensitive information or intellectual property. To accomplish this, devices must use extremely low power. They also must be housed in tamper-reactive packages that include suitable interfaces for the variety of sensors used to create this security fence around content-sensitive circuitry.

It is important to realize that the strength of an encryption algorithm is no longer the target of an attack. It is much easier and far more beneficial to simply devise clever ways to steal the keys. Therefore, an increasing amount of attention is being placed upon physical hardware protection requirements.

Emerging Security Standards

Most newly evolving security standards stem from specifications set forth by the National Institute of Standards and Technology (NIST) in the US and from the Communications Electronics Security Group (CEG) in the UK. These organizations provided standards known as FIPS 140-1 and ITSEC, respectively.

Because of the many new standards emerging and increasing level of security required, these and other multinational groups are adopting a new single standard that combines the best of these standards, known as "Common Criteria" (see *Appendix 2—Common Certifications/Standards*). For example, NIST has now updated its FIPS specification to 140-2 and will soon be moving solely to Common Criteria.

With the increasing proliferation of devices capable of conducting financial transactions, other standards now come into play. Among the most recognized is EMV (European MasterCard® Visa®) and PCI PED (payment card industry; PIN entry device), which was established by MasterCard and Visa. One can expect these certification standards to become increasingly more stringent due to the newly evolving trends associated with DRM, the ability for mobile platforms to conduct financially related transactions while protecting a user's or system's identity, and new government initiatives such as FIPS 201 Personal Identity Verification (PIV).

All of the aforementioned standards outline the physical security requirements that must be met for certification for various end-equipment categories. Generally, this requires security to be addressed in multiple layers beginning at the silicon-processor level and ending at the packaging that surrounds the processor, memory, or data path exposed to sensitive content or algorithms. For an end product to achieve certification, it must undergo extensive testing by an approved laboratory and be accompanied by a security target document that outlines how specific physical security threats are mitigated. In the case of some standards (PCI, for example), the manufacturer must show what security improvements have been made over their existing products to meet newly updated criteria. In many instances, the vague nature of exactly how security must be designed into a product can be very frustrating to manufacturers and design teams who have not yet had to face these types of requirements.

The requirements that determine what level of security certification is needed vary considerably; nonetheless, the demands placed upon physical tamper protection are becoming increasingly more stringent. These demands are driven by the availability of sophisticated analysis tools and the technical expertise necessary to launch a sophisticated attack.

Introducing the DeepCover Security Manager Product Family

To assist designers' ever-increasing need for physical security while reducing size, cost, and power consumption, Maxim announced the first in a series of security controllers that specifically addresses the needs of increased physical hardware protection. The DeepCover® Security Manager (DS3600), the first in this product family, gives embedded-systems designers the ability to add the additional layers of security required for present and emerging certification requirements.

These devices have sophisticated temperature monitoring for extremely low-leakage current comparators, protection against cryogenic attacks, time-keeping and tamper-logging functions, and a host of other functions required by cryptographic subsystems (**Figure 1**). At the hub of this array of functionality lies a unique memory-cell structure intended to further protect top-level encryption keys and security certificates. Traditional memory-cell technology is subject to phenomena called data imprinting, which refers to a memory cell's trait of leaving remnants of previously stored information. These remnants can be extracted through a variety of attack scenarios. The DS3600's internal nonimprinting memory is the first device of its kind to eliminate this common point of attack. Additionally, the entire memory array can be erased with a single hardware command instantaneously. This security controller's combination of functionality dramatically reduces power consumption and no longer requires host processor intervention for the protection of encryption key memory.

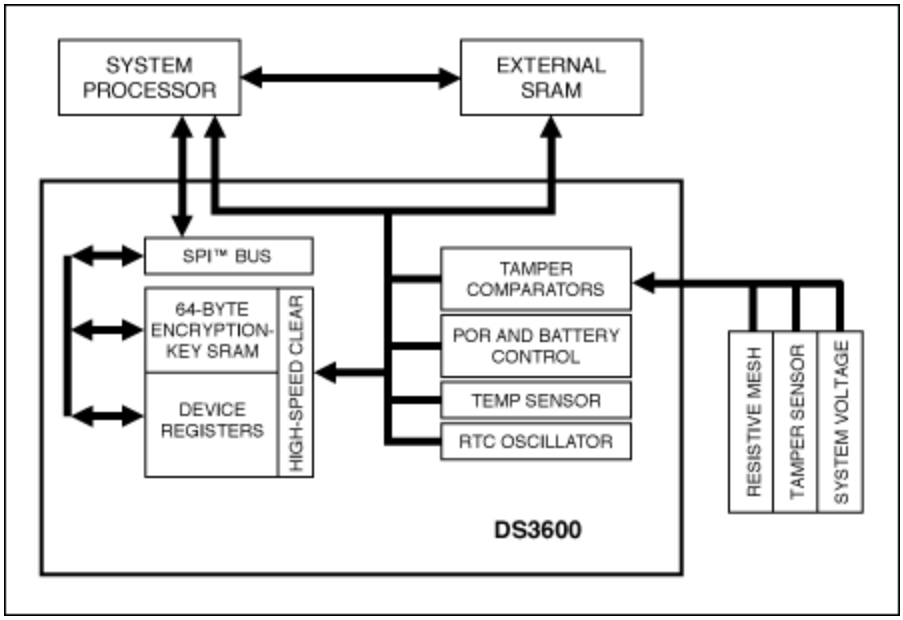

Figure 1. The tamper-resistant DS3600 controller features extremely high-impedance comparators to provide continuous low-power system monitoring and meet the highest level Common Criteria requirements.

In many cases, the highly integrated features found in this family of controllers have replaced the functionality of over 40 discrete components. While reducing size and cost at a fraction of the power traditionally required, the DS3600 family can virtually eliminate the need for other expensive components such as secure microprocessors. This allows manufacturers of embedded systems based upon non-secure processor architectures to achieve certification and retain large intellectual property software assets. Because these devices have been designed to meet certification, they provide the most assistance for designers who must now produce the necessary documentation for product certification.

Appendix 1—Classification Taxonomy

To determine the level of security required, IBM® presented a classification taxonomy over a decade ago that is still used today to describe potential attack classifications.

Class I (Clever Outsiders)

- Often very intelligent
- Have insufficient knowledge of the system
- May have access to moderately sophisticated equipment
- Typically attack a weakness in the system, rather than create one

Class II (Knowledgeable Insiders)

- Have substantial specialized technical education and experience
- Have some system knowledge, but potential access to most of it
- Often have access to sophisticated tools and instruments for analysis

Class III (Funded Organizations)

- Possess nearly unlimited funding resources
- Able to assemble teams of specialists
- Able to acquire or gain access to the most advanced analysis tools
- Capable of in-depth analysis and design of sophisticated attacks
- May recruit Class II knowledgeable insiders as part of the attack team

At a minimum, a system designer seeking to achieve certification should be able to describe the threats associated with at least the following common attack scenarios.

Physical Attacks

- Package intrusion
  - Cutting, etching, and ion or laser drilling
  - Reverse engineering (requires several sample devices)
    - Generating circuit schematics
    - Extracting ROM code
    - Identifying physical location of key circuit elements (i.e., memory)
  - Gaining access to memory
    - Alter circuitry with an FIB workstation
    - Alter the state of specific transistors with ionizing radiation
    - Microprobing
    - Advanced spectrographic analysis of memory-cell oxides

Noninvasive Attacks

- Ionizing radiation and thermal/cryogenic
- Induced voltage fluctuations and clock disturbance
- Differential power analysis

Appendix 2—Common Certifications/Standards

NIST FIPS 140-2 Levels 1 to 4

- CSEG ITSEC E1 to E6
- Common Criteria EAL1 to EAL7
- EMV 4.1 Levels 1 to 2 (Primarily Used in Banking/POS)
- ZKA (Primarily Used in Banking/POS)
- PCI PED (Primarily Used in Banking/POS PIN Entry

Industry Moving Towards "Common Criteria" Unification

- Various protection profiles, security targets, and schemes can exist
- UK EN45011:1998
- ISO-15408
- Trusted computer group provides additional protection profiles
- IBM Trusted Mobile Platform security

These and other standards bodies are summarized below, along with a brief description of related security levels.

NIST FIPS 140-2

FIPS 140-2 defines four levels of security assurance, from lowest to highest, with each level building on the previous one.

Level 1 means that the product properly implements the NIST standardized cryptographic algorithms, including data encryption standard (DES), triple DES (3DES), and advanced encryption standard (AES).

Level 2 means that the product has tamper-evident coatings to ensure that any corruption of the device would be noticeable.

Level 3 is for cryptographic modules that delete stored keys if the modules detect a physical attack on circuit components. At Level 3, the product must require authenticated access.

Level 4 requires that a product provide protection from attacks that attempt to thwart physical access controls, such as supercooling.

Most security products receive FIPS 140-2 Level 2 or Level 3 certification, either of which is sufficient as long as the modules are contained in a controlled environment.

Common Criteria

Common Criteria uses a scale called evaluation assurance level (EAL). This is an assessment that says that the product meets the functional requirements stated in the security target and protection profile documents. These documents are prepared by the vendor and evaluated by the Common Criteria evaluator. EAL levels range from EAL1 to EAL7, with most products receiving Common Criteria certification of EAL4 and below.

EAL1 Product meets the basic requirements.

EAL7 Product meets the requirements for exceptionally secure environments.

EAL5, 6, and 7 certifications are extremely stringent, requiring evaluation of the development process and theoretical framework, as well as functional tests.

An EAL rating is meaningless without first evaluating the security target and protection profile documentation.

A similar article appeared in the October 2006 issue of *Embedded Systems Europe*.

Related Parts		
DS3600	DeepCover Security Manager with 64B Nonimprinting, Battery-Backed Encryption Key SRAM	Free Samples
DS3605	DeepCover Security Manager for NV SRAM Control with RTC and Thermal Tamper Detection	Free Samples
DS3640	DeepCover Security Manager with I²C Interface and 1KB Nonimprinting Battery-Backed Encryption Key SRAM	Free Samples
DS3641	DeepCover Security Manager with SPI-Compatible Interface and 1KB Nonimprinting Key Memory	Free Samples
DS3644	DeepCover Security Manager with 1KB Secure Memory and Programmable Tamper Hierarchy	Free Samples
DS3645	DeepCover Security Manager with 4KB Secure Memory and Tamper Protection	Free Samples
DS3650	DeepCover Security Manager with Thermal Tamper Detection	Free Samples
DS3655	DeepCover Security Manager with Ultra-Low-Power Tamper Detection and Nonimprinting Memory	Free Samples
DS3660	DeepCover Security Manager for Low-Voltage Operation with 1KB Secure Memory and Programmable Tamper Hierarchy	
MAX36025	DeepCover Security Manager for Tamper-Reactive Cryptographic-Node Control with AES Encryption	
MAX36051	DeepCover Security Manager with 128 Bytes of	

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 3976: http://www.maximintegrated.com/an3976
APPLICATION NOTE 3976, AN3976, AN 3976, APP3976, Appnote3976, Appnote 3976