Understanding security features for MSP430™ Microcontrollers

Texas Instruments

Security problem targeted: Typical threats / security measures

MSP430 MCUs are optimized for sensing and measurement embedded applications across different industrial markets including building automation, grid infrastructure, test and measurement, factory automation, medical, health and fitness and personal electronics. Below are a few examples of typical attacks on select applications and what MSP430 MCUs provide to help mitigate the risks.

- Eavesdrop or impersonate communication within a smart meter application
  - Encrypt communications with MSP430 AES accelerators
- Physically tamper with E-meter boxes to fool billing software
  - Detect tampers and record timestamps of intrusion with the MSP430 RTC_C (Real Time Clock "C") module
- Manipulate firmware updates to handheld devices to compromise systems
  - Provide an additional layer of security for firmware updates with an MSP430 bootstrap loader (BSL) password protection and the crypto-bootloader
- Clone blood glucose meter algorithms through unauthorized access of JTAG or code injection
  - Mitigate risk of intrusion by locking the JTAG and using MSP430 IP encapsulation available on some FRAM devices

Family description

MSP430™ microcontrollers (MCUs) from Texas Instruments (TI) are 16-bit mixed-signal processors designed for ultra-low-power sensing and measurement applications. TI MSP430 MCUs enable some of the lowest power-sensing and measurement applications with a variety of integrated peripherals. TI also provides all of the hardware and software tools you need to get started today. Learn more at **www.ti.com/msp**.

TI Embedded Security Portfolio –

Security is hard, TI makes it easier

Security features details:

MSP430 MCU security features coupled with ultra-low-power operation can enable embedded designers to address the following security objectives:

- **Physical security** is a requirement in embedded systems in order to prevent tampering of the system. MSP430 devices that have an RTC_C module include a security feature to detect and record physical tamper attempts in all MCU low-power modes (LPMs). These dedicated input pins are typically connected to an external mechanical switch to detect when an enclosure is opened. It could also be connected to a PCB wire or wire mesh to detect unauthorized access. When an event occurs, the time and date of the event are recorded into a battery backup memory. In addition, if enabled within the code, it triggers an interrupt so further actions may be taken. Some examples where this type of detection would be implemented are: an MCU-based electricity meter (e-meter), smart thermostat or control panel. In the metering case the system would typically be connected to a mechanical switch to detect any physical attempt to bypass the meter at the terminal block enclosed within the housing.
- **IP protection** is a requirement in most embedded systems, and in microcontroller systems this correlates to protecting the software IP stored in embedded memory. MSP430 MCUs provide the means to either lock the JTAG access using a password or to disable it by programming a fuse signature. In cases where the JTAG is disabled, access to the device is possible only using the bootstrap loader (BSL). The BSL requires a password to read out or program the device. On all

Security enablers

The family of MSP430 MCUs includes a variety of security features; these may be embedded within the device hardware, programmed during device manufacture or implemented as part of the user's program code.

Security enablers	Device	Detailed security features	Learn more
Debug security	**All MSP430 families**	**Credential protection** Offers increased protection against unauthorized access to the device through the debug interface. JTAG security fuse/lock or FRAM password	**MSP430 Programming Via the JTAG Interface User's Guide**
Cryptographic acceleration	**MSP430FR59xx/69xx**	**256-bit AES hardware accelerator** Enables increased security for data transfers via the integrated hardware security accelerator while saving power by drastically reducing the cycles required for symmetric encryption/decryption	**MSP430FRxx User's Guide** (See AES accelerator chapter)
	MSP430F5xx/F6xx, CC430		**MSP430F5xx/6xx, CC430** User's Guides
	MSP430FR59xx/69xx	**True random number seed** Generate random AES keys, and do so more often with FRAM-based devices	**MSP430FRxx User's Guide** (See 1.14.3.4 Random Number Seed) **Random Number Generation Using MSP430FR59xx and MSP430FR69xx MCUs**
Software IP protection	**MSP430FR59xx/69xx**	**IP encapsulation** Segregate your proprietary software from the rest of the application	**MSP430FRxx User's Guide** (See 7.2.2 IP Encapsulation Segment) **MSP Code Protection Features**
Secure firmware and software update	**All MSP430 families**	**BSL password protection** Password-protected BSL commands to guard against unauthorized device access	**MSP430 Programming Via the Bootstrap Loader (BSL) User's Guide**
	MSP430FR59xx/69xx	**Crypto-bootloader (software solution)** Offers increased protection against critical threats to field firmware update mechanisms with authentication and encryption of new firmware image	**Crypto-Bootloader – Secure in-field firmware updates for ultra-low-power MCUs** **Secure In-Field Firmware Updates for MSP MCUs**
Physical security	**MSP430F677x**	**Tamper I/O with RTC time stamp** Two pins can be used as an event or tamper-detection input of an external switch (mechanical or electronic), with an RTC time stamp	**MSP430F5xx/6xx User's Guide** (see 24.3.2 Real-Time Clock Event/Tamper Detection with Time Stamp)

TI offers security enablers to help developers implement their security measures to protect their assets (data, code, identity and keys).

FRAM-based and many Flash-based MSP430 devices, providing an incorrect BSL password will result in a mass erase of the FRAM or Flash. Some FRAM devices support an IP Encapsulation (IPE) feature. The IPE module protects a programmed portion of memory from read or write access from anywhere outside of the IP Encapsulated area, even by JTAG. Execution of this portion of memory can be limited to specific callback functions that are defined at the time the IPE module is enabled. This IPE module minimizes risk of exposure of critical or proprietary software from the rest of the application, making it harder for a malicious third party to reverse-engineer the sensitive software code. For more information and best practices, please see **MSP Code Protection Features**, section 3 *IP Encapsulation (IPE).*

- **Secure communication** in connected systems (remote or local) is essential to protect data communicated between parties. Cryptographic algorithms are primarily used to maintain confidentiality and integrity of the data in transit and to verify authenticity of the data upon reception. Many MSP430 devices include a powerful yet efficient hardware accelerator designed for **AES encryption / decryption** (128-, 192- and 256-bit key length). This accelerator offers greater than 40 times cycle reduction compared to regular C implementations. Several FRAM devices also include a random number stored within the memory of the device, which provides a seed for a deterministic random number generator. This number is generated on the production test system using a cryptographic random number generator and is

programmed during production test of the device. Software libraries for commonly used **cryptography algorithms including AES, DES, 3-DES, SHA-2** are also available for MSP430 MCUs.

- **Secure firmware updates** are increasingly needed within embedded systems to allow designers to provide secure service and support their products that are already deployed in the field. In most cases, this translates into guarding against reverse-engineering of new firmware image and verifying firmware integrity and authenticity before it's programmed into the device. For MSP430 FRAM MCUs (MSP430FR58xx/59xx), the crypto-bootloader can provide an increased layer of security for firmware updates supporting authentication and encryption of new firmware images. Embedded peripherals such as the AES module form the basis of a **crypto-bootloader solution for select MSP430 FRAM MCUs**. This can help designers mitigate risks against several types of attacks, which if successful could lead to a loss of proprietary software or enable a system to be hijacked.

Additional resources

- **MSP430 Programming with the JTAG Interface User's Guide**
- **MSP430FRxx User's Guide** (see AES accelerator chapter)
- **MSP430F5xx/6xx**, **CC430** User's Guides
- **MSP430FRxx User's Guide** (see 1.14.3.4 Random Number Seed)
- **Random Number Generation Using MSP430FR59xx and MSP430FR69xx MCUs**
- **C Implementation of Cryptographic Algorithms**
- **MSP430FRxx User's Guide** (see 7.2.2 IP Encapsulation Segment)
- **MSP Code Protection Features**
- **MSP430 Programming Via the Bootstrap Loader (BSL) User's Guide**
- **Crypto-Bootloader – Secure in-field firmware updates for ultra-low-power MCUs**
- **Secure In-Field Firmware Updates for MSP MCUs**
- **MSP430F5xx/6xx User's Guide** (see 24.3.2 Real-Time Clock Event/ Tamper Detection With Time Stamp)
- **System-Level Tamper Protection Using MSP MCUs**

Security is hard, TI makes it easier

For more information about TI's Embedded Security Solutions, visit **www.ti.com/security**

IMPORTANT NOTICE FOR TI DESIGN INFORMATION AND RESOURCES

Texas Instruments Incorporated ('TI") technical, application or other design advice, services or information, including, but not limited to, reference designs and materials relating to evaluation modules, (collectively, "TI Resources") are intended to assist designers who are developing applications that incorporate TI products; by downloading, accessing or using any particular TI Resource in any way, you (individually or, if you are acting on behalf of a company, your company) agree to use it solely for this purpose and subject to the terms of this Notice.

TI's provision of TI Resources does not expand or otherwise alter TI's applicable published warranties or warranty disclaimers for TI products, and no additional obligations or liabilities arise from TI providing such TI Resources. TI reserves the right to make corrections, enhancements, improvements and other changes to its TI Resources.

You understand and agree that you remain responsible for using your independent analysis, evaluation and judgment in designing your applications and that you have full and exclusive responsibility to assure the safety of your applications and compliance of your applications (and of all TI products used in or for your applications) with all applicable regulations, laws and other applicable requirements. You represent that, with respect to your applications, you have all the necessary expertise to create and implement safeguards that (1) anticipate dangerous consequences of failures, (2) monitor failures and their consequences, and (3) lessen the likelihood of failures that might cause harm and take appropriate actions. You agree that prior to using or distributing any applications that include TI products, you will thoroughly test such applications and the functionality of such TI products as used in such applications. TI has not conducted any testing other than that specifically described in the published documentation for a particular TI Resource.

You are authorized to use, copy and modify any individual TI Resource only in connection with the development of applications that include the TI product(s) identified in such TI Resource. NO OTHER LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE TO ANY OTHER TI INTELLECTUAL PROPERTY RIGHT, AND NO LICENSE TO ANY TECHNOLOGY OR INTELLECTUAL PROPERTY RIGHT OF TI OR ANY THIRD PARTY IS GRANTED HEREIN, including but not limited to any patent right, copyright, mask work right, or other intellectual property right relating to any combination, machine, or process in which TI products or services are used. Information regarding or referencing third-party products or services does not constitute a license to use such products or services, or a warranty or endorsement thereof. Use of TI Resources may require a license from a third party under the patents or other intellectual property of the third party, or a license from TI under the patents or other intellectual property of TI.

TI RESOURCES ARE PROVIDED "AS IS" AND WITH ALL FAULTS. TI DISCLAIMS ALL OTHER WARRANTIES OR REPRESENTATIONS, EXPRESS OR IMPLIED, REGARDING TI RESOURCES OR USE THEREOF, INCLUDING BUT NOT LIMITED TO ACCURACY OR COMPLETENESS, TITLE, ANY EPIDEMIC FAILURE WARRANTY AND ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF ANY THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

TI SHALL NOT BE LIABLE FOR AND SHALL NOT DEFEND OR INDEMNIFY YOU AGAINST ANY CLAIM, INCLUDING BUT NOT LIMITED TO ANY INFRINGEMENT CLAIM THAT RELATES TO OR IS BASED ON ANY COMBINATION OF PRODUCTS EVEN IF DESCRIBED IN TI RESOURCES OR OTHERWISE. IN NO EVENT SHALL TI BE LIABLE FOR ANY ACTUAL, DIRECT, SPECIAL, COLLATERAL, INDIRECT, PUNITIVE, INCIDENTAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES IN CONNECTION WITH OR ARISING OUT OF TI RESOURCES OR USE THEREOF, AND REGARDLESS OF WHETHER TI HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

You agree to fully indemnify TI and its representatives against any damages, costs, losses, and/or liabilities arising out of your non-compliance with the terms and provisions of this Notice.

This Notice applies to TI Resources. Additional terms apply to the use and purchase of certain types of materials, TI products and services. These include; without limitation, TI's standard terms for semiconductor products http://www.ti.com/sc/docs/stdterms.htm), evaluation modules, and samples (http://www.ti.com/sc/docs/sampterms.htm).

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265