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.

This IPE module mini- mizes 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 AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATA SHEETS), DESIGN RESOURCES (INCLUDING REFERENCE DESIGNS), APPLICATION OR OTHER DESIGN ADVICE, WEB TOOLS, SAFETY INFORMATION, AND OTHER RESOURCES “AS IS” AND WITH ALL FAULTS, AND DISCLAIMS ALL WARRANTIES, EXPRESS AND IMPLIED, INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT OF THIRD PARTY INTELLECTUAL PROPERTY RIGHTS.

These resources are intended for skilled developers designing with TI products. You are solely responsible for (1) selecting the appropriate TI products for your application, (2) designing, validating and testing your application, and (3) ensuring your application meets applicable standards, and any other safety, security, regulatory or other requirements.

These resources are subject to change without notice. TI grants you permission to use these resources only for development of an application that uses the TI products described in the resource. Other reproduction and display of these resources is prohibited. No license is granted to any other TI intellectual property right or to any third party intellectual property right. TI disclaims responsibility for, and you will fully indemnify TI and its representatives against, any claims, damages, costs, losses, and liabilities arising out of your use of these resources.

TI’s products are provided subject to TI’s Terms of Sale or other applicable terms available either on ti.com or provided in conjunction with such TI products. TI’s provision of these resources does not expand or otherwise alter TI’s applicable warranties or warranty disclaimers for TI products.

TI objects to and rejects any additional or different terms you may have proposed.

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