

S. Mione

Are you looking for a secure way to update firmware in the field? Do you know why you need security for in-field firmware updates?

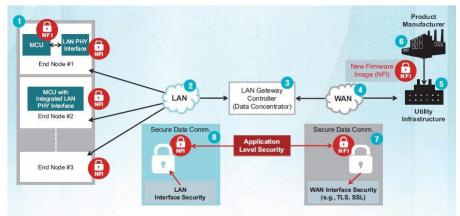


Figure 1: Example representation of network-connected MCUs in-field firmware updates

In-field firmware updates are becoming an increasingly popular feature supported on products that are deployed to the field, especially Internet of Things (IoT) applications. The updates enable new firmware images to be downloaded into the microcontroller's (MCU's) memory. This gives product manufacturers a way to offer service and support to products already deployed in the field.

However, this feature is also very commonly exploited by attackers, and if vulnerable, can compromise the security of the system. In-field firmware updates are one of the first targets for attackers looking to compromise the security of a system. The consequences could include: loss of intellectual property and product cloning, all the way to complete control of the deployed system.

MSP430[™] MCU's recently released an authenticated encryption solution called Crypto-Bootloader for increasing the security of in-field firmware updates in ultra-low-power MSP microcontrollers like the MSP430FR59xx/69xx MCU families. We made sure to offer more security without compromising memory. The implementation of Crypto-Bootloader in an MSP430FRx MCU takes only 3.2 KB of code and less than 1 KB of data space!

Ready to take a look at the software solution? The Crypto-Bootloader solution provides the following tools for in-field firmware update processes:

- Bootloader Scripter Tool (MSPBSL): User interface which enables communication with the BSL on MSP microcontrollers to modify the device's memory via UART, I2C, SPI or USB.
- Crypto-Bootloader for MSP430FR5x/6x FRAM MCUs: This bootloader uses cryptographic functions to enable increased security for in-field firmware updates. A Graphical User Interface (GUI) is available for a simplified user-experience.
- **Microcontroller Bootloader Programming Board (MSP-BSL):** Hardware interface providing a bridge between the PC's USB port and UART, I2C or SPI.

Visit the links below to learn more about Crypto-Bootloader and your security options:

- · Learn more about Crypto-Bootloader secure in-field firmware updates
- Check out the Crypto-Bootloader training series

1



• Buy the Bootloader for MSP low-power microcontrollers

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 Copyright © 2023, Texas Instruments Incorporated