Understanding security features for SimpleLink™ MSP432E4 ethernet MCUs

MCU for industrial gateway

The SimpleLink™ MSP432™ (MSP432E4xx) Ethernet microcontrollers (MCU) are based on a 120 MHz Arm® Cortex®-M4 core with floating-point capabilities and integrate a 10/100 Ethernet MAC and PHY. The MSP432E4 MCUs support an unparalleled number and combination of wired connectivity interface. The SimpleLink MSP432E4 Ethernet MCU and the SimpleLink software development kit (SDK) enable developers to accelerate intelligent gateway designs by harnessing its advanced integration, wireless connectivity plug-ins and unified tool chain.

With a breadth of advanced, integrated wired communication peripherals, including the Ethernet, the SimpleLink MSP432E4 MCUs allow developers to connect to more sensors and control more actuator edge nodes without sacrificing price, performance, or power consumption. The hardware security accelerators and the ample computing power enable the MSP432E4 to function as an industrial embedded gateway to aggregate and analyze sensor data prior to cloud communication. Furthermore, the SimpleLink SDK enables the merging of wired and wireless connectivity to meet a wide range of connectivity requirements.

Security problem targeted: Typical threats/ security measures

Network connectivity can expose the gateways and end-nodes to increased security threats via remote and local-area-network accesses. The “security assets” in the system can include code, data or keys and can be compromised at any of the “exposure points” including storage, runtime or transfer. Data communicated over the network may contain user confidential information or sensor data that may be used for billing purposes or firmware image used to for software updates. It is important to secure this communication data as much as possible to enable data confidentiality, integrity, authenticity and in many cases non-repudiation attributes. Remote threats can also compromise device data/code confidentiality or modify device operation or system behavior.

Additionally, the gateways and end-nodes can be vulnerable to physical threats including an attacker trying to access debug port or attempting to physically tamper the device to extract local security assets. Compromising security assets local to the product may have direct financial impact in many applications and furthermore, can be used to perform more sophisticated attacks over the network.

Intellectual property (IP) thefts that enable product cloning and manipulation are other prominent threats to embedded systems. It could lead to compromising trade secrets of embedded system developers and enable cloned software/products with inferior safety and reliability standards.

Security enablers:

The MSP432E4 MCUs offer a variety of security enablers, consisting of features embedded within the device hardware, programmed during device manufacture and implemented as part of the user’s program code.

Device	Security enablers	Detailed security features
MSP432E401Y MSP432E411Y	Device identity	128-bit unique device identifier
	Debug security	Permanent debug lock. Device factory reset disables debug security
	Cryptographic acceleration	• AES hardware accelerator: o 128-, 192, 256-bit support o ECB, CBC, CTR, CFB, F8, F9, GCM, CCM, XTS modes support • DES and 3-DES o ECB, CBC, CFB support • MD5, SHA-1, SHA-2 (SHA-224, SHA_256) o HMAC key processing support
	Physical security	Tamper module with mechanisms to detect, respond to, and log system tampering events.
	SW IP protection	Flash memory region protection
	Network security	mbedTLS software library using device cryptographic acceleration is available as part of MSP432E4 SDK.

For more information about the TI Security Solutions, visit the TI security web site at www.ti.com/security

Security features details:

The MSP432E4 MCUs offer a varied set of security enablers to help developers design products with increased security to detect, protect and mitigate security risks to their system.

- Secure data communication in connected systems (remote or local) is essential to allow data to be communicated between valid parties maintaining the following security attributes: confidentiality, integrity, authenticity (and non-repudiation in many cases). This requires securing the communication data at various network communication model layers.
    - **The cryptographic accelerators** on MSP432E4 support *AES, DES/3DES and MD5, SHA-1,2 (with HMAC key processing support)* operations to enable performing crypto operations in a faster and power optimized way. These cryptographic accelerators enable security attributes essential for data confidentiality, integrity, and authenticity.
- As part of **network security** at the session layer, TLS/SSL security can be applied for enabling client to server communication security. mbedTLS software library that enables this capability is available with the MSP432E4 SDK. The mbedTLS library uses HW cryptographic accelerators available on the MSP432E4 devices. Additionally, the software library supports asymmetric cryptographic functions essential for key exchanges without sharing secret keys in plaintext, authentication using digital signatures and for enabling non-repudiation as a security attribute for communication data.
- **Device identity** involves each device programmed with a *128-bit unique device identifier* at TI production programming. This identifier is stored in read-only system control module.
- **Debug security** enables locking debug access to device permanently. The debug lock can be unlocked only with a factory reset process that erases all user application firmware and security settings on-chip before enabling the device debug access.
- **Physical security** is enabled by the *on-chip tamper module* that has mechanisms to detect, respond to, and log system tampering events. The Tamper module is designed to be low power and operate either from a battery or the MCU I/O voltage supply. It supports up to 4 tamper inputs (for example, to detect case open/close detect or interface to other external tamper sensors) and includes long and short glitch filters to qualify the tamper input conditions. It also supports external oscillator tamper detection. Tamper responses include clearing hibernate SRAM memory and recording tamper log with timestamp for up to 4 tamper events. These features should be leveraged to put together a system level tamper solution for the product.
- As a second layer, the MCUs offer flash protections such as read-only, in 2-kB increments, and execute-only, in 16-kB increments, mechanisms to help the user protect the integrity and confidentiality of software IPs stored in these protected regions (security enabler: Software IP Protection).

Additional resources

SimpleLink MSP432 SDK

- mbed TLS is part of the SimpleLink MSP432E4 SDK

MSP432E4 as an Intelligent Gateway:

- "Building a gateway from the sensors to the cloud" white paper
- SimpleLink MSP432E4 Gateway to Cloud training video
- "Merging wired and wireless connectivity to build an intelligent gateway to the cloud" blog post

- "System-Level Tamper Protection Using MSP MCUs" **application note**

For more information about the TI Security Solutions, visit the TI security web site at www.ti.com/security

© 2019 Texas Instruments Incorporated
Printed in U.S.A.

IMPORTANT NOTICE AND DISCLAIMER

TI PROVIDES TECHNICAL AND RELIABILITY DATA (INCLUDING DATASHEETS), 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, 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 (www.ti.com/legal/termsofsale.html) 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.

Mailing Address: Texas Instruments, Post Office Box 655303, Dallas, Texas 75265
Copyright © 2019, Texas Instruments Incorporated