X-CUBE-SBSFU security evaluation method description

Introduction

In 2017, STMicroelectronics introduces the X-CUBE-SBSFU STM32Cube Expansion Package, a free reference software package under SLA to help STM32 users to design their Secure Boot (SB) and Secure Firmware Update (SFU) solution. The X-CUBE-SBSFU Expansion Package allows the update of the STM32 microcontroller built-in program with new firmware versions, adding new features and correcting potential issues. The update process is performed in a secure way to prevent unauthorized updates and access to confidential on-device data such as secret code and firmware encryption key.

In addition, Secure Boot checks and activates the STM32 hardware security mechanisms, and checks the authenticity and integrity of the user application code before every execution to ensure that invalid or malicious code cannot be run (see the UM2262 user manual).

The X-CUBE-SBSFU Expansion Package is composed of several modules, which are implemented depending on the STM32 mechanisms they offer:

- Secure Boot module
- Secure Firmware Update module
- Secure engine module
- Key management service module (only for the STM32L4 Series and STM32WL Series)

1 Description

To verify the source code of the software modules in X-CUBE-SBSFU, STMicroelectronics requested a security assessment of all the X-CUBE-SBSFU reference software to an external laboratory. SGS-Brightsight has been selected to evaluate the X-CUBE-SBSFU software.

This security evaluation aims at verifying the robustness of the code shared on the market; It is not intended to be used for certification reference but rather for STMicroelectronics to show platform security benefits to its customers and differentiate from its competitors.

The STM32 mechanisms are studied on four different groups of microcontrollers after their embedded hardware protection. These groups include the following STM32 microcontroller series:

- STM32G0 Series, STM32G4 Series, STM32H7 Series
- STM32F4 Series, STM32F7 Series, STM32L1 Series
- STM32L0 Series, STM32L4 Series, STM32L4+ Series
- STM32WB Series, STM32WL Series

The security evaluation checks the combination of software and hardware blocks to provide confidentiality and authenticity to the user application and the capability to securely update it. The evaluation focuses on the security of the X-CUBE-SBSFU software modules against logical and external perturbation attacks assuming full control of the user and external loader applications.

The code review focuses on single- and dual-image configurations. The code review includes neither the STMicroelectronics cryptographic library X-CUBE-CRYPTOLIB nor other supported external open-source cryptographic libraries such as mbedTLS or mbed-crypto.

Perturbation, side-channel, and logical attacks are considered during the X-CUBE-SBSFU software global code review.

- Perturbation attacks consist in single fault perturbation attacks using basic equipment and board-level manipulations.
- Side-channel attacks consist in extracting the secrets of cryptographic operations using electromagnetic emanations or power consumption measurements of the targeted operation. Note that none of the verified STM32 hardware accelerators support side-channel robustness. Specialized cryptographic library or clearly specified STM32 hardware accelerators available on secure STM32 microcontrollers must be used to become resistant against side channel attacks.
- For logical attacks, the logical vulnerability robustness of the X-CUBE-SBSFU software is verified, aiming at checking the software coding rules and protection of the code against common exploits. Conditional test and access, buffer manipulation, memory clearing, and secure assets access are the types of logical issues that are verified.

This global security assessment program done on the X-CUBE-SBSFU STM32Cube MCU Package allows users looking to develop a secure device to start their design from a trusted software base. It is part of the STM32Trust security framework deployed by STMicroelectronics on STM32 microcontrollers.

2 X-CUBE-SBSFU recommendations

The external evaluation conclusion is that the product offers a reasonable level of security backed up by the hardware features. The following points must be considered by the final solution developer:

- The integrator must follow the recommendations in the integration guide (see the AN5056 application note).
- The solution must be deployed in RDP level 2 or physical countermeasures must be deployed to prevent unauthorized debugging in level 1.
- The integrator must individualize the SBSFU keys for each device and preserve the confidentiality of private and secret keys.
- The integrator must be careful when modifying the secure engine module, as a vulnerability in this module could lead to compromising the whole solution.

In addition to these global recommendations, which can be applicable to all the microcontroller series compatible with X-CUBE-SBSFU, specific points must be considered during the application development. For further information and support, contact the local STMicroelectronics office.

3 References

The documents listed in Table 1 are part of the reference technical documentation used for X-CUBE-SBSFU security evaluation.

Table 1. Security evaluation reference documents

Identifier	Title	Type	Revision[1]
AN5056	Integration guide for the X-CUBE-SBSFU STM32Cube Expansion Package	Application note	5
UM2262	Getting started with the X-CUBE-SBSFU STM32Cube Expansion Package	User manual	7
RM0090	STM32F405/415, STM32F407/417, STM32F427/437 and STM32F429/439 advanced Arm®-based 32-bit MCUs	Reference manual	18
RM0410	STM32F76xxx and STM32F77xxx advanced Arm®-based 32-bit MCUs	Reference manual	4
RM0444	STM32G0x1 advanced Arm®-based 32-bit MCUs	Reference manual	2
RM0440	STM32G4 Series advanced Arm®-based 32-bit MCUs	Reference manual	3
RM0455	STM32H7A3/7B3 and STM32H7B0 Value line advanced Arm®-based 32-bit MCUs	Reference manual	3
RM0377	Ultra-low-power STM32L0x1 advanced Arm®-based 32-bit MCUs	Reference manual	8
RM0038	STM32L100xx, STM32L151xx, STM32L152xx and STM32L162xx advanced Arm®-based 32-bit MCUs	Reference manual	16
RM0351	STM32L47xxx, STM32L48xxx, STM32L49xxx and STM32L4Axxx advanced Arm®-based 32-bit MCUs	Reference manual	6
RM0434	Multiprotocol wireless 32-bit MCU Arm®-based Cortex®-M4 with FPU, Bluetooth® Low-Energy and 802.15.4 radio solution	Reference manual	8
RM0453	STM32WL5x advanced Arm®-based 32-bit MCUs with sub-GHz radio solution	Reference manual	1

1. *The document revision used for the evaluation may differ from the document revision available on STMicroelectronics website at www.st.com.*

Note: Arm is a registered trademark of Arm Limited (or its subsidiaries) in the US and/or elsewhere.

Revision history

Table 2. **Document revision history**

Date	Revision	Changes
24-Nov-2021	1	Initial release.