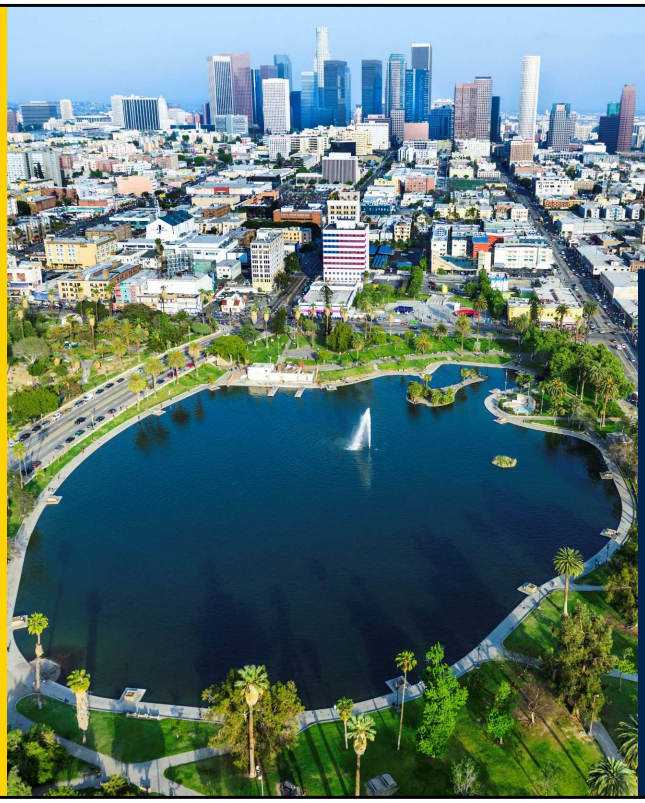


life.augmented

STM32U0 – Security-Memory protections

Hello and welcome to this presentation of the STM32U0 security protections. It will cover the different means for protecting code and data.

Overview

- Purposes:
  - Provide read and write protection of embedded firmware and data in:
    - Flash memory
    - SRAM2
    - Backup registers
  - Provide secure execution of sensitive firmware

APPLICATION BENEFITS

- Protection of STM32 embedded software intellectual property
- Prevents hacking or dumping code through a JTAG interface or other possible means of external attack
- Protects code/data from unwanted/accidental erasure (i.e. loader, calibration data)
- Allows development of secure applications (secure boot or secure firmware update…)

life.augmented

Memory protections have been designed for different purposes.
Protected memories are the flash memory, SRAM2 and the backup registers.
A read protection, for example, will prevent the dumping of embedded software code through an external access and will protect the developer's intellectual property.
A write protection will prevent certain flash sectors from being accidentally erased by a load overflow in a software or data update procedure.
STM32U0 microcontrollers provide several features for protecting code and data located in flash memory, SRAM2 and backup registers.
The following slides will describe all these protection features.

Key features

- **Readout protection (RDP)**
  - Global protection of flash memory, SRAM2 and backup registers against external access
  - Memories and registers are protected from SWD/JTAG access when boot is different from user flash memory
  - Three RDP levels defined from no protection to full and permanent protection
- **Write protection (WRP)**
  - Flash memory sectors protection against write/erase/program access
  - Flash memory code with write protection attribute is protected against unwanted write or erase operations

Protection depends on the RDP level

Request	Permission
Read	YES
Write	**NO**
Execute	YES

life.augmented

The following means are provided for code protection purposes:
RDP: ReaDout Protection
WRP: Write protection
An external access can be gained by using a JTAG connector, a Serial Wire port or the boot software embedded in SRAM.
Three levels of RDP protection are defined from Level 0, which offers no protection at all, to Level 2 which has full and permanent protection.
The write protection mechanism prevents accidental or malicious write/erase operations.

Key features

- **Securable Memory Area (HDP)**
  - Flash memory area protection with specific access mechanisms for sensitive firmware execution
  - Code and data in this area are only accessible after reset
  - Boot code is executed prior to any other process
  - After transition, the area is closed and cannot be accessed until the next reset

Request	Permission
Boot read	YES
Application read	NO
Boot write	YES
Application write	NO
Boot execute	YES
Application execute	NO

life.augmented

Secure User Memory protection ensures the safe execution of sensitive applications in addition to code and data protection.
Secure User memory is a Flash memory area with a specific protection mechanism to ensure the safe execution of sensitive firmware in addition to code and data protection.
The HDP acronym stands for Hide Protection.
All protection mechanisms are configurable via the STM32U0 option bytes.
Once the secure boot has been executed, the Secure User Memory is no longer accessible until the next reset.

STM32U0 flash related protection features

	STM32U0
Number of banks	1
Page size	2-KB
Write Protect areas (WRPs) ➢ Page granularity	2
Securable memory area ➢ Page granularity ➢ Starts at the first pages of the memory	1

life.augmented

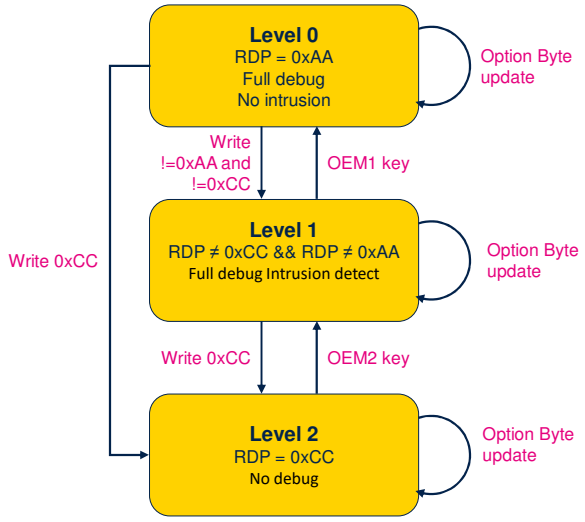
5

The features regarding memory protection supported by the STM32U0 are:

- One flash bank
- Page size of 2 kilobyte
- Two write protect areas
- One securable memory area.

Readout protection

- The read protection is activated by setting the RDP option byte and then, by applying a system reset to reload the new RDP option byte
- The read protection protects the main flash memory, the option bytes, and the backup registers
- There are three levels of read protection from no protection (level 0) to maximum protection or no debug (level 2)



life.augmented

This slide shows the possible transitions between each readout protection level. It is always possible to raise the protection level, but regression can be disabled.
When the RDP is reprogrammed to the value 0xAA to move from Level 1 to Level 0, a mass erase of the Flash main memory is performed.
Backup registers and SRAM2 are also erased.
The OTP area is not affected by mass erase and remains unchanged.
Note that the RDP level is coded in one option byte; Level 0 is coded by a 0xAA value, Level 2 is coded by a 0xCC value and Level 1 is coded by any value other than 0xAA or 0xCC.

Readout protection

Protection levels 0 and 1

- RDP Level 0
  - No protection is set, all operations (Read / Program / Erase) are permitted on Flash memory, SRAM2, and backup registers
  - Option bytes can be modified
- RDP Level 1
  - No access (read, erase, program) to Flash memory and backup registers can be performed while the debug port is connected or while booting from RAM or **system** flash memory bootloader
    - A bus error is generated in case of a read or write request
  - Access to protected memories from user code are allowed when booting from **user** flash memory
  - Option bytes can be modified and protection level regression to Level 0 is possible, but this causes the Flash memory, the SRAM2 and backup registers to be mass-erased

life.augmented

7

When the lowest RDP level, Level 0, is set, the device has no protection.
All read or write operations (if no write protection is set) on the flash memory, the SRAM2 and the backup registers are possible in all boot configurations (such as flash user boot, debug or boot from RAM).
Option bytes are also changeable in this level.
Level 0 is the factory default level.
In Level 1, read protection is set for the Flash memory, SRAM2 and the backup registers.
In this level, protected memories are only accessible when booting from user flash memory.
Whenever a debugger access is detected, or boot is not set to a user Flash memory area, any access to the protected memories generates a system hard fault which blocks all code execution until the next power-on reset.

Note that option bytes can still be modified in this level, making it possible to remove the protection.

Readout protection

Level regression and Protection level 2

- Protection level regression from Level 1 to Level 0
  - Mass erase of Flash memory, SRAM2 and backup registers
    - Protected areas (Secure User memory) may be kept unchanged depending on their erase policy
  - Option bytes and OTP bytes are not erased
- RDP Level 2
  - All protections provided by Level 1 are active and permanent
  - Option bytes can no longer be changed, internally or externally
  - SWD/JTAG is disabled
  - Boot from RAM or System memory (boot loader) are no longer allowed
  - Only boot in user Flash memory is allowed and enables all operations (R/W/Erase) on the Flash memory and backup registers

life.augmented

8

We have seen in the previous slide that it is possible to modify option bytes in Level 1. It is then possible to remove the protection by changing the protection level to Level 0.
This protection level regression will cause the Flash memory, the SRAM2 and the backup registers to be mass-erased.
Flash areas configured as Secure User Memory can be erased or left unchanged depending on their erase policy configuration.
Readout protection Level 2 provides the same protection as in Level 1, but the protection can become permanent.
When the protection level 2 is active, the Debug port, the boot from RAM and the boot from system memory are disabled.
This level must only be considered in the final product

when the development stage is completed.
Note that to ensure that there are no backdoors, this protection cannot be bypassed even at ST factory.

Readout protection

- Two 128-bit keys (OEM1KEY and OEM2KEY) can be defined and used to lock the RDP regression

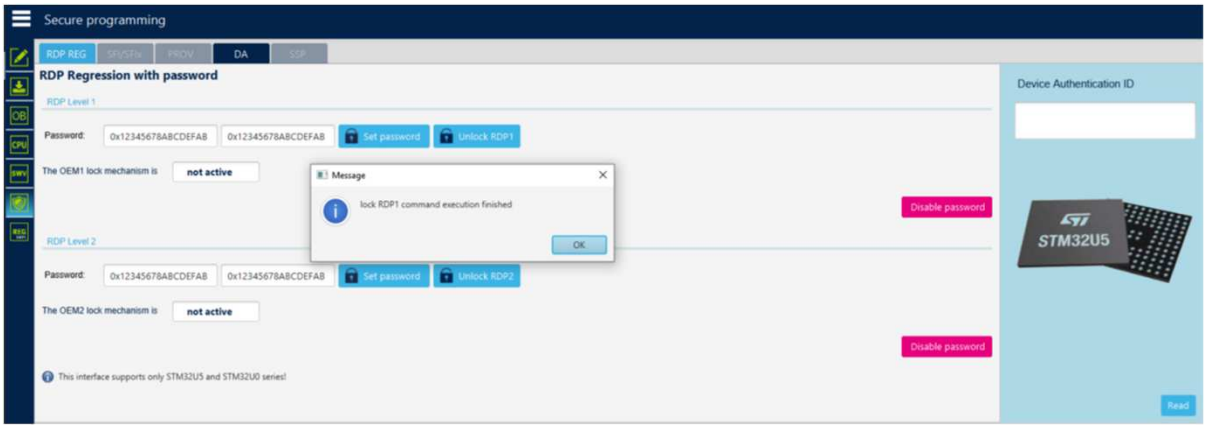
Key	Description
OEM1 KEY	When the OEM1 RDP lock mechanism is active, it **blocks** the RDP level 1 to RDP level 0 regression
OEM2 KEY	When the OEM2 RDP lock mechanism is active, it **allows** the RDP level 2 to RDP level 1 regression

life.augmented

The read protection is using regression mechanism with user-defined passwords called OEM keys.
The OEM key size is 128bit.
For regression, keys must be written to the debug interface registers under reset.
After applying OEM2 key, the regression is done by hardware when reset signal raises.
After applying OEM1 key, the option byte can be programmed for regression.
The use of OEM keys is optional.

Readout protection
Regression using the STM32CubeProgrammer

- Secure programing section of CubeProgrammer manages password and unlock
  - Unlock process must be done in access port 1, in hot-plug
  - OB regression can then be finished after switching to access port 0



life.augmented

The regression can be configured and used either by the command line interface tools, which is ideal for automated scripts, or using the Cube Programmer graphical interface, which is friendly for first contact and experimentation.
To comply with security constraints, some steps require connecting to specific access port or under hot-plug mode.

Readout protection

Summary

Area	Protection level (RDP)	Access rights when Boot in User Flash memory	Access rights when Boot from RAM or from bootloader or Debug Access detected
Main Flash memory	1	R/W/E	No Access
	2	R/W/E	N/A, only boot in user flash memory is allowed
System Flash memory (Boot loader)	1	R	R
	2	R	N/A, only boot in user flash memory is allowed
Option bytes	1	R/W/E	R/W/E
	2	R	N/A, only boot in user flash memory is allowed
Backup registers	1	R/W	No Access
	2	R/W	N/A, only boot in user flash memory is allowed
SRAM2	1	R/W	No Access
	2	R/W	N/A, only boot in user flash memory is allowed
OTP	1	R/W	No Access
	2	R/W	N/A, only boot in user flash memory is allowed

W: Write R: Read E: Erase

life.augmented

11

This table summarizes the different types of access authorized for the Flash memory and backup registers according to the readout protection (or RDP) level, configured boot mode and with debug access, as seen in previous slides.
The system memory is only read-accessible, whatever the protection level (0, 1 or 2) and execution mode.

Flash memory write protection

Protects code and data from unwanted or accidental erasure

- Write protection attributes
  - Protected sectors cannot be erased or programmed
- Setting/resetting
  - Protection is set independently for each page of the Flash memory
  - Protection is set in option byte registers
  - Write protection can be reset freely in RDP Level 0
    - It can only be modified in RDP Level 1 or Level 2 when user flash memory was used for boot
  - If any page is write-protected, the mass erase does not work
    - Write protection must be removed prior to a level regression associated with flash memory mass erase

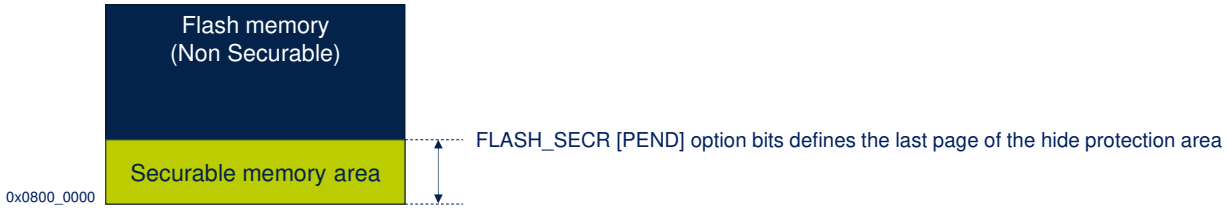
life.augmented

The write protection protects code and non-volatile data from unwanted or accidental erasure.
This protection is only available on the Flash memory.
The write protection can be set on a selection of Flash memory pages only.
When a page is protected, it cannot be erased or programmed.
Any attempt to write-access the sector will cause a Flash memory error.
If at least one page is write-protected, a mass-erase of the Flash memory cannot be performed.
The protection needs to be removed first.

Securable memory area (HDP)

Introduction

- The main purpose of the securable memory area is to protect a specific part of Flash memory against undesired access
  - This allows implementing software security services such as secure key storage or secure boot



  - When FLASH_SECR[HDP1EN] option bits are equal to 0xB4, securable memory is not configured

life.augmented

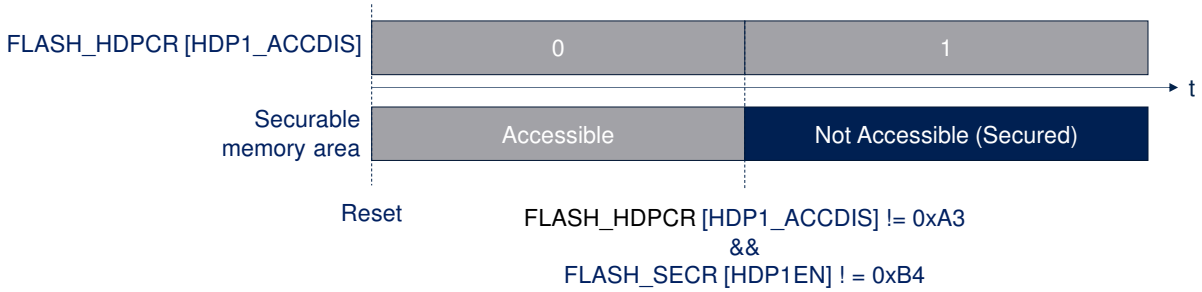
13

The purpose of the securable memory is to store code and data, available during the boot time, that become inaccessible once the boot program sets a control bit.
The typical use case consists in performing an authentication and possibly decryption of the software image present in the flash memory by using cryptographic keys contained in the securable memory. The authentication and decryption programs are also stored in the securable memory.
Option bits are used to set the size of the securable memory in page units. Base address is always 0x0800_0000 which corresponds to Cortex-M0+ reset vectors.
Therefore, before activating the securable memory area, move the vector table outside the page 0.
When the HDP1EN field in the option bytes is equal to

0xB4, securable memory is not implemented.

Securable memory area

- By default, after a reset, the securable memory is accessible
  - Once the HDP1_ACCDIS byte is set to a value different than 0xA3, the securable memory becomes inaccessible until the next reset



life.augmented

14

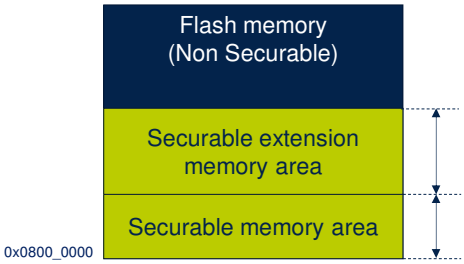
When secured, any write access (programming, erase) to the securable memory area is rejected and generates a bus error.
Fetch and read accesses return zero (read-as-zero RAZ).
The securable area can only be unsecured by a system reset.
In case of secure boot, used to perform image authentication and decryption, set the condition to transition to secured state when the authentication is successful, just before branching to the first instruction of the image.
This condition depends on two settings:

- Register's field FLASH_HDPCR [HDP1_ACCDIS] disables HDP1 area access when it is different than 0xA3
- Option byte FLASH_SECR [HDP1EN] disables HDP

area when it is different than 0xB4.

When set to a value different from 0xA3, FLASH_HDPCR [HDP1_ACCDIS] cannot be modified except by a system reset.

Securable memory area Extension



FLASH_HDPEXTR[HDP1_EXT] register field defines the size of the extension area

FLASH_SECR [PEND] option bits defines the last page of the hide protection area

- FLASH_HDPCR[HDP1EXT_ACCDIS] enables access to the extension area when value is equal 0xA3

HDP1EXT_ACCDIS value	HDP1EXT_ACCDIS access	HDP1_EXT access	Flash sectors covered accessible
0xA3	OK	OK	Yes
0x5C	OK, if written value is not 0xA3	OK to write higher value	No
Any other	WI	WI	No

life.augmented

15

The HDP1 area can be extended through HDP1_EXT of the FLASH HDP extension register. This is a new feature offered by the STM32U0.
HDP1_EXT indicates the number of pages added to the HDP area.
The start page offset of the HDP1 extension area depends on the presence of an HDP1 area.
If there is an HDP1 area, the HDP1 extension area starts from HDP1_PEND + 1.
Otherwise, it starts from the user flash memory base address.
The value HDP1EXT_ACCDIS field determines the access to the extension area, and the possibility of changing the size of the extension area:

- When equal to 0xA3, access to the extension area is permitted and updates of HDP1_EXT field are

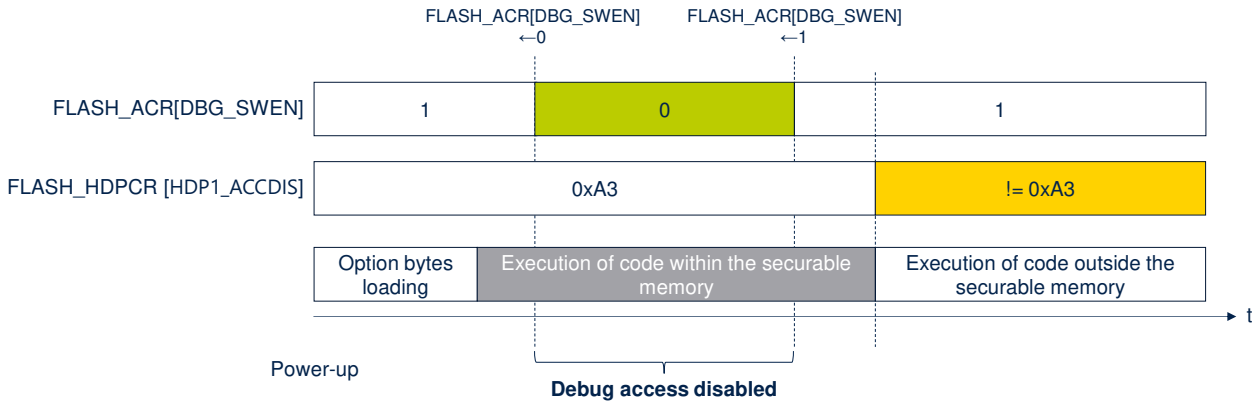
supported

- When equal to 0x5C, access to the extension area is denied, but HDP1_EXT field can be updated
- When different than 0xA3 and 0x5C, access to the extension area is denied and HDP1_EXT field cannot be updated.

Note that HDP1EXT_ACCDIS field itself cannot be programmed to 0xA3 when it is equal to 0x5C and cannot be reprogrammed at all when its value is different than 0xA3 and 0x5C.

Disabling core debug access

- For executing sensitive code or manipulating sensitive data in securable memory area, the debug access to the core can temporarily be disabled



life.augmented

16

Taking control of the Cortex-M0+ by using invasive debug can be temporarily disabled by programming appropriately the DBG_SWEN control bit.
For instance, the secure boot can decide to clear this bit before performing authentication/decryption and then to set this bit to one to re-enable invasive debug once the authentication is successful.
Once the securable memory is secured, it is no longer accessible from software running in the microcontroller and from debugger.

Forcing boot from Flash memory

- STM32U0 boot memories:
  - Embedded SRAM
  - System memory (bootloader)
  - Main Flash memory
- To increase the security and establish a chain of trust, the BOOT_LOCK option bit of the FLASH_SECR register allows forcing the system to boot from the Main Flash memory regardless the other boot options
  - It is always possible to set the BOOT_LOCK bit
  - Conditions to reset this bit:
    - RDP is set to Level 0, or
    - RDP is set to Level 1, while Level 0 is requested, and a full mass-erase is performed

life.augmented

17

In the STM32U0, three different boot modes can be selected: boot from embedded SRAM, boot from system memory and boot from main Flash memory.
Executing a secure boot from securable memory implies that the boot area is the Flash memory.
To disable the other boot areas, the BOOT_LOCK option bit has to be set in the FLASH_SECR register.
This option bit can be set unconditionally.
However, resetting is possible only when RDP level is zero or RDP is changed from Level 1 to Level 0, which causes a full mass-erase.

Related peripherals

- Refer to this training related to this peripheral:
  - STM32U0- Flash memory

life.augmented

Please refer to the Flash memory training to learn more about the memory architecture, option bytes and Flash memory operations.

Thank you

life.augmented

Thank you for attending this presentation!