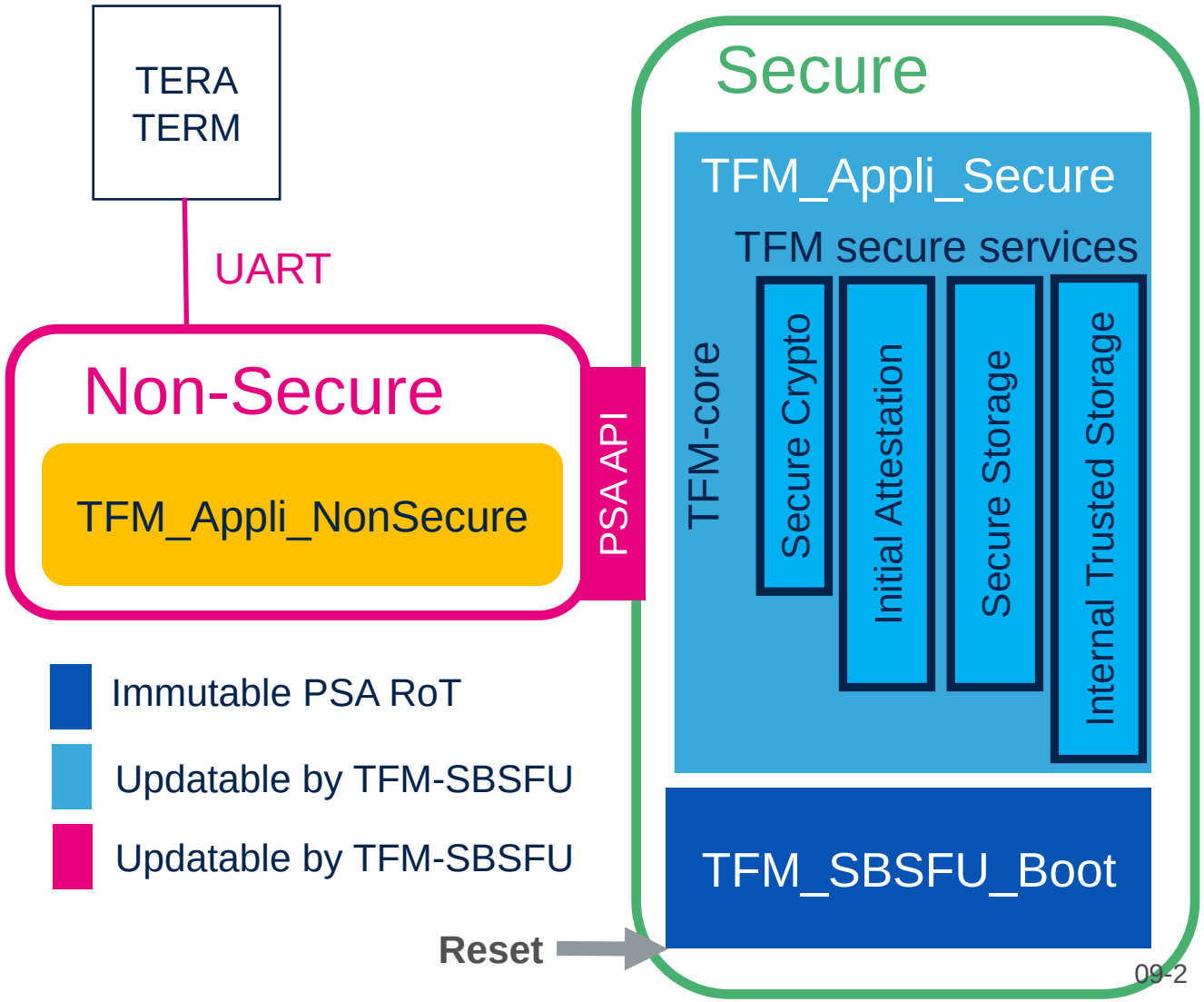
life.augmented

STM32 Security Workshop

PSA-TFM Hands-on

L5-TFM hands-on

- Purpose :
  - Understand the L5 TFM structure
  - Test TFM-SBSFU
  - Experiment with L5 security features
- Hands-on scenario (45 minutes)
  - Experiment SBSFU functionalities: Update TFM Appli Secure + TFM Appli NonSecure over UART
  - Compile and debug
  - Activate HDP
  - Activate RDP 0.5



Material provided

- Port of the TFM from STM32L562E-DK to NUCLEO-L552ZE-Q
  - Migration from UART1 to LPUART 1
  - Deactivated features : External memory support / TFM local loader
  - Remove crypto hardware acceleration as not available on STM32L552E
  - Tested with CubeIDE 1.4.2 + STM32Cube_FW_L5_V1.3.0
  - Deactivate some default security flags (WRP / HDP / RDP)

C:\STM32SecuWS\TFM\STM32Cube_FW_L5_V1.3.0\Projects\NUCLEO-L552ZE-Q\Applications\TFM_for_WS

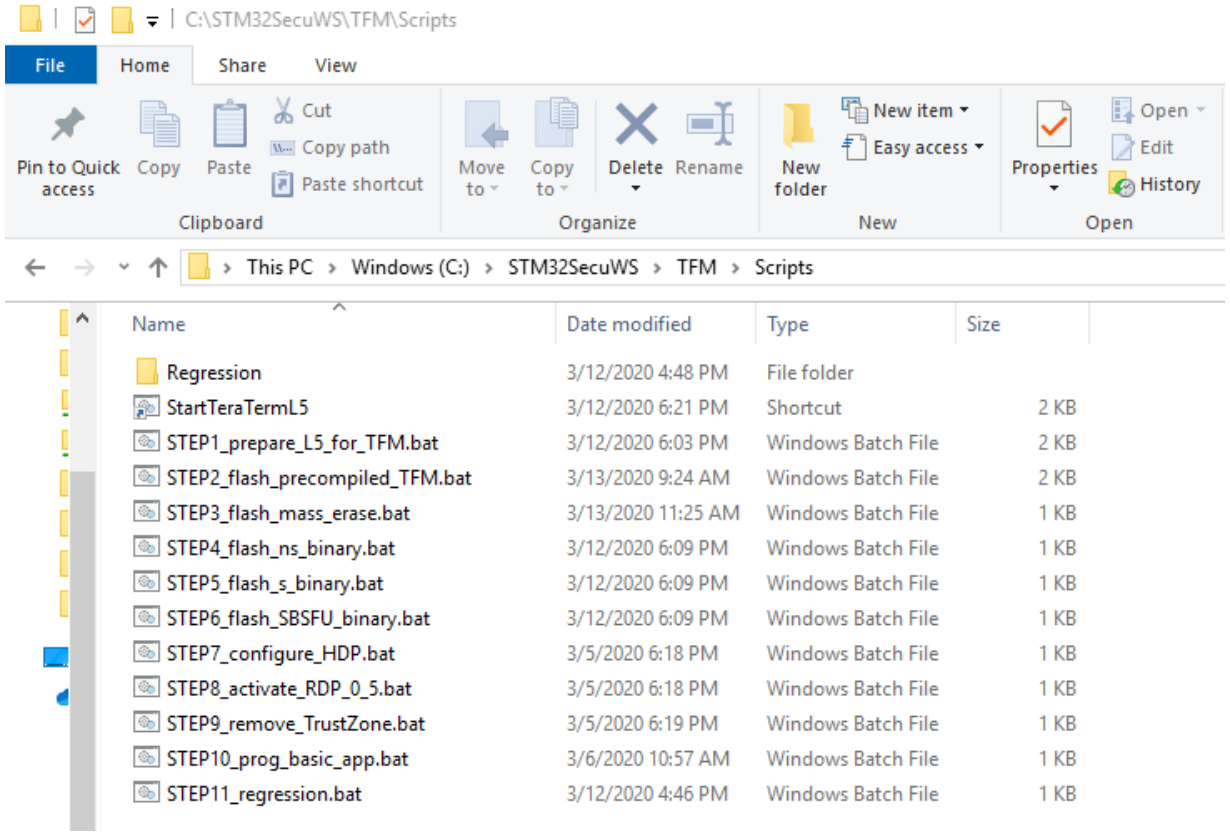
- Delivery some bat script for modifying option byte and flash binaries
  - They rely on CubeProgrammer tools which should be available at this path C:\Program Files\STMicroelectronics\STM32Cube\STM32CubeProgrammer\bin\STM32_Programmer_CLI.exe

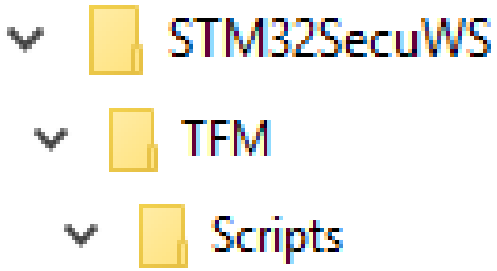
C:\STM32SecuWS\TFM\Scripts

Experiment SBSFU functionalities

Open an explorer dedicated to scripts

- During this hands-on we will use scripts
- Please keep an explorer window open to access rapidly to these scripts:



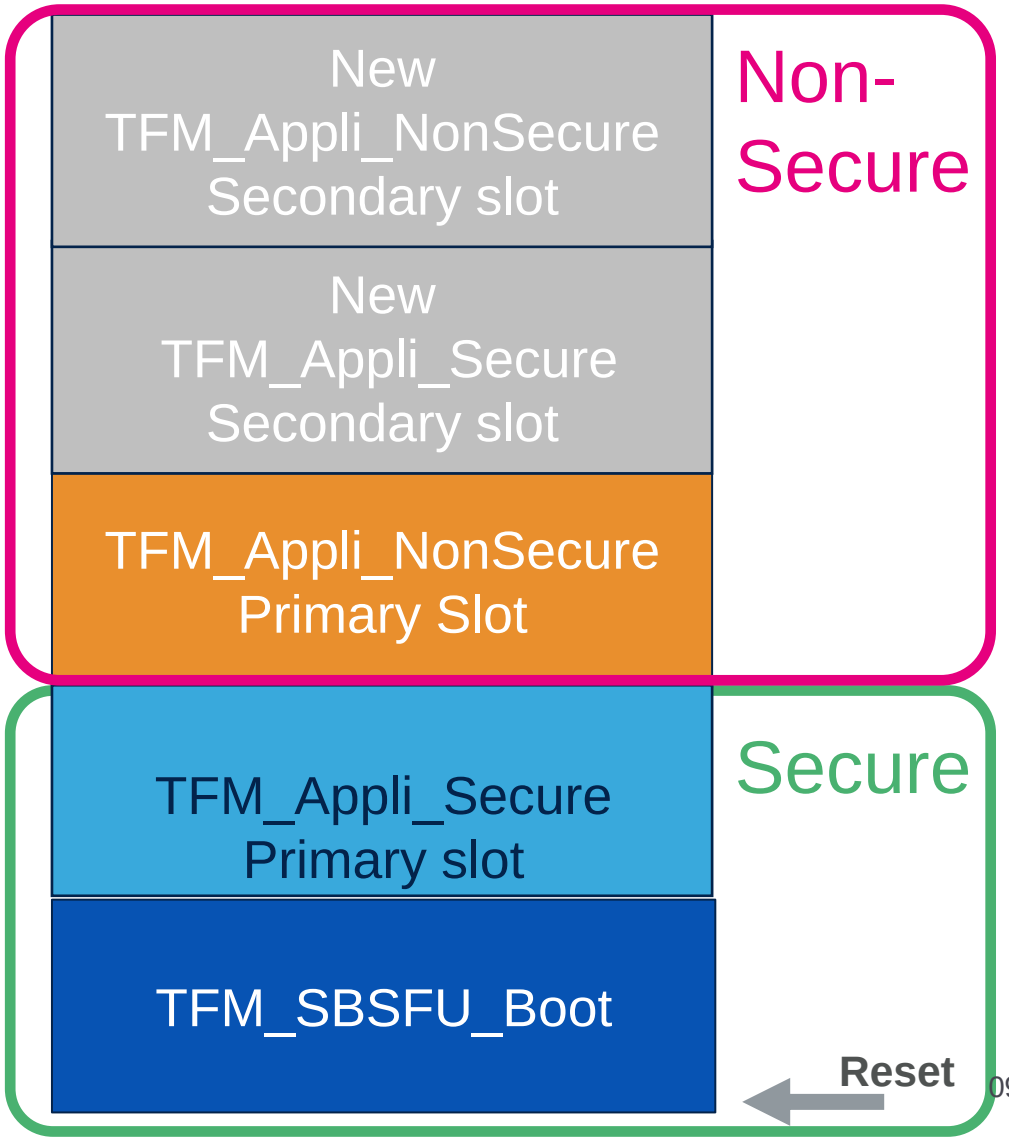


TFM-Nucleo L5 Flash memory map

- Two slots for both Secure and Non-Secure App
- Secure split of flash must reflect placement of slots and TFM-SBSFU
- Modify Option bytes (Flash WaterMark)
- Please launch and check the traces :

  STEP1_Prepare_L5_for_TFM.bat

Some warning as DBank and TZEN already set by previous hands-on…



life.augmented

```
C:\windows\system32\cmd.exe
  Bank           : 0x00
  Address        : 0x50022040
  Size           : 32 Bytes

                                                  100%

  Bank           : 0x01
  Address        : 0x50022060
  Size           : 16 Bytes

                                                  100%

OPTION BYTE PROGRAMMING VERIFICATION:

Option Bytes successfully programmed

"*****************************************************************"
"Option setting"
"*****************************************************************"
"TZ           : enabled "
"SRAM2_RST    : disabled "
"SECBOOTADD0 : 0x180032 -> 0x0C001900"
"DBANK        : enabled "
"SECWM1_PSTRT: 0x0      -> 0x08000000"
"SECWM1_PEND : 0x6F     -> 0x08037800"
"SECWM2_PSTRT: 0x7f     -> 0x0803f800"
"SECWM2_PEND : 0x00     -> 0x08000000"
"*****************************************************************"
"Board is ready to receive the TFM binaries, press key"
Press any key to continue . . .
```

- You could ignore : Warning: Option Byte: xxxx, value: 0xx, was not modified (those option byte has been already set in the previous hands-on)

life.augmented

Flash the TFM software

- First flash precompiled version of TFM

  TFM_Appli_NonSecure + associated metadata : tfm_ns_sign.bin

  TFM_Appli_Secure + associated metadata : tfm_s_sign.bin

  TFM_SBSFU_Boot : TFM_SBSFU_Boot.bin

- **C:\STM32SecuWS\TFM\Scripts**
- Please launch :
  - STEP2_flash_precompiled_TFM.bat

Flash the TFM software

C:\windows\system32\cmd.exe

```
Memory Programming ...
Opening and parsing file: tfm_ns_sign.bin
  File          : tfm_ns_sign.bin
  Size          : 28196 Bytes
  Address       : 0x08038000


Erasing memory corresponding to segment 0:
Erasing internal memory sectors [112 125]
Download in Progress:
                                                  100%

File download complete
Time elapsed during download operation: 00:00:01.127



Verifying ...


Read progress:
                                                  100%

Download verified successfully


"TFM_Appli NonSecure Written, press a key to flash the TFM_Appli Secure"
Press any key to continue . . .
```

1 Press any key

C:\windows\system32\cmd.exe

```
Memory Programming ...
Opening and parsing file: tfm_s_sign.bin
  File          : tfm_s_sign.bin
  Size          : 138812 Bytes
  Address       : 0x0C014000


Erasing memory corresponding to segment 0:
Erasing internal memory sectors [40 107]
Download in Progress:
                                                  100%

File download complete
Time elapsed during download operation: 00:00:05.237



Verifying ...


Read progress:
                                                  100%

Download verified successfully


"TFM_Appli Secure Written, press a key to flash the "
Press any key to continue . . .
```

2 Press any key

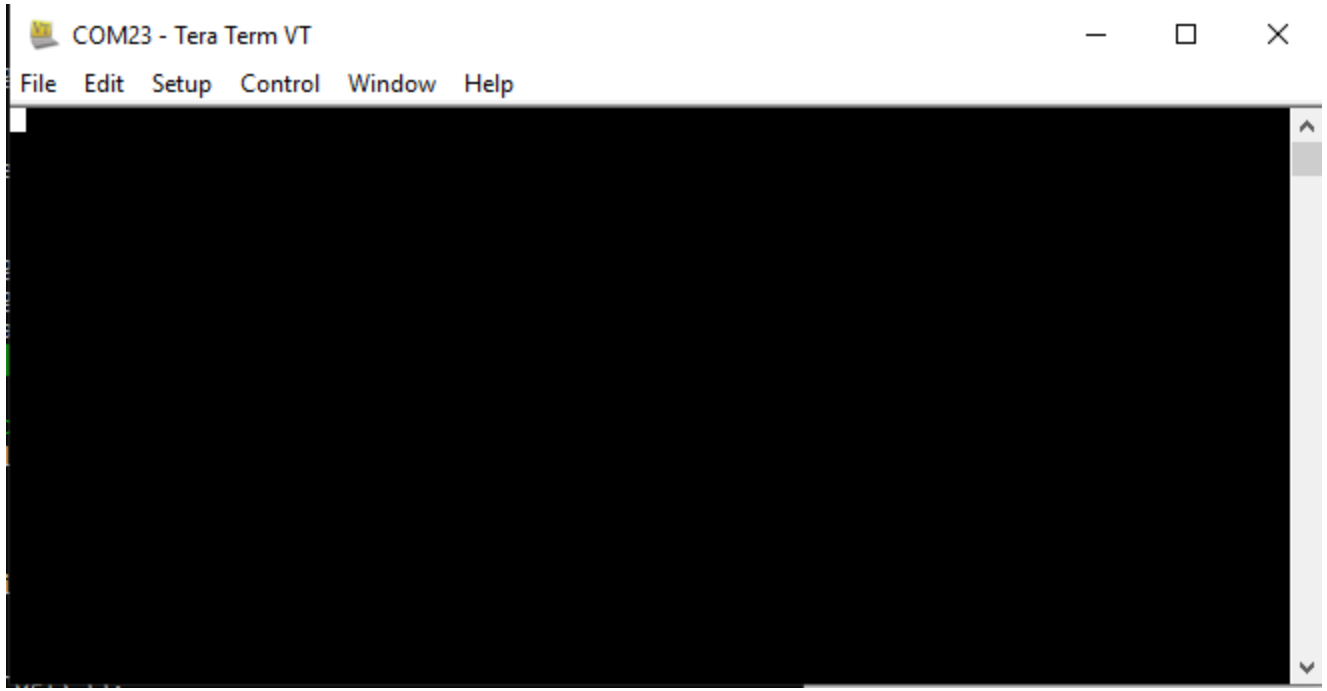
C:\windows\system32\cmd.exe

```
Memory Programming ...
Opening and parsing file: TFM_SBSFU_Boot.bin
  File          : TFM_SBSFU_Boot.bin
  Size          : 55930 Bytes
  Address       : 0x0C001000


Erasing memory corresponding to segment 0:
Erasing internal memory sectors [2 29]
Download in Progress:
                                                  100%

File download complete
Time elapsed during download operation: 00:00:02.158



Verifying ...


Read progress:
                                                  100%

Download verified successfully


"TFM SBSFU Done, press a key"
Press any key to continue . . .
```

3 Press any key

Flash the TFM software

- Then launch TeraTerm us the script :
  - StartTeraTermL5



- Reset the board

Check the TFM traces on the Teramterm

```
[INF] Starting bootloader
[INF] Initializing BL2 NV area : Power down/reset not supported...
[INF] Init BL2 NV Header area: Done
[INF] Initializing BL2 NV Counters
[INF] Init BL2 NV counters to 0 : Done
[INF] BL2 NV Area Initialized : Power Down/reset supported
[INF] Checking BL2 NV area
[INF] Checking BL2 NV area header
[INF] Checking BL2 NV Counter consitency
[INF] Consistent BL2 NV Counter 3  = 0x0
[INF] Consistent BL2 NV Counter 4  = 0x0
[INF] Swap type: none
[INF] Swap type: none
[INF] verify counter  0 1000000 0
[INF] counter  0 : ok
[INF] verify sig key id 0
[INF] signature OK
[INF] Counter 3 set to 0x1000000
[INF] verify counter  1 1000000 0
[INF] counter  1 : ok
[INF] verify sig key id 1
[INF] signature OK
[INF] Counter 4 set to 0x1000000
[INF] Bootloader chainload address offset: 0x14000
[INF] Jumping to the first image slot
[INF] BL2 HUK _STM32L652XX_HUK_CUSTOMIZATION_
 set to BL2 SHARED DATA
[INF] Code c001900 c00ea7a
[INF] hash TFM_SBSFU_Boot  8b114fc3 .. 87de87c
[Sec Thread] Secure image initializing!

=====================================================================
=              (C) COPYRIGHT 2019 STMicroelectronics                =
=                                                                   =
=                          User App #A                              =
=====================================================================


=================== Main Menu ============================

  Test Protections ------------------------------------- 1

  Test TFM --------------------------------------------- 2

  Download a new Fw Image ------------------------------ 3

  Selection :
```

TFM_SBSFU traces

TFM_Appli_Secure traces

TFM_Appli_NonSecure traces

life.augmented

Download new firmware menu

COM20 - Tera Term VT

File Edit Setup Control Window Help

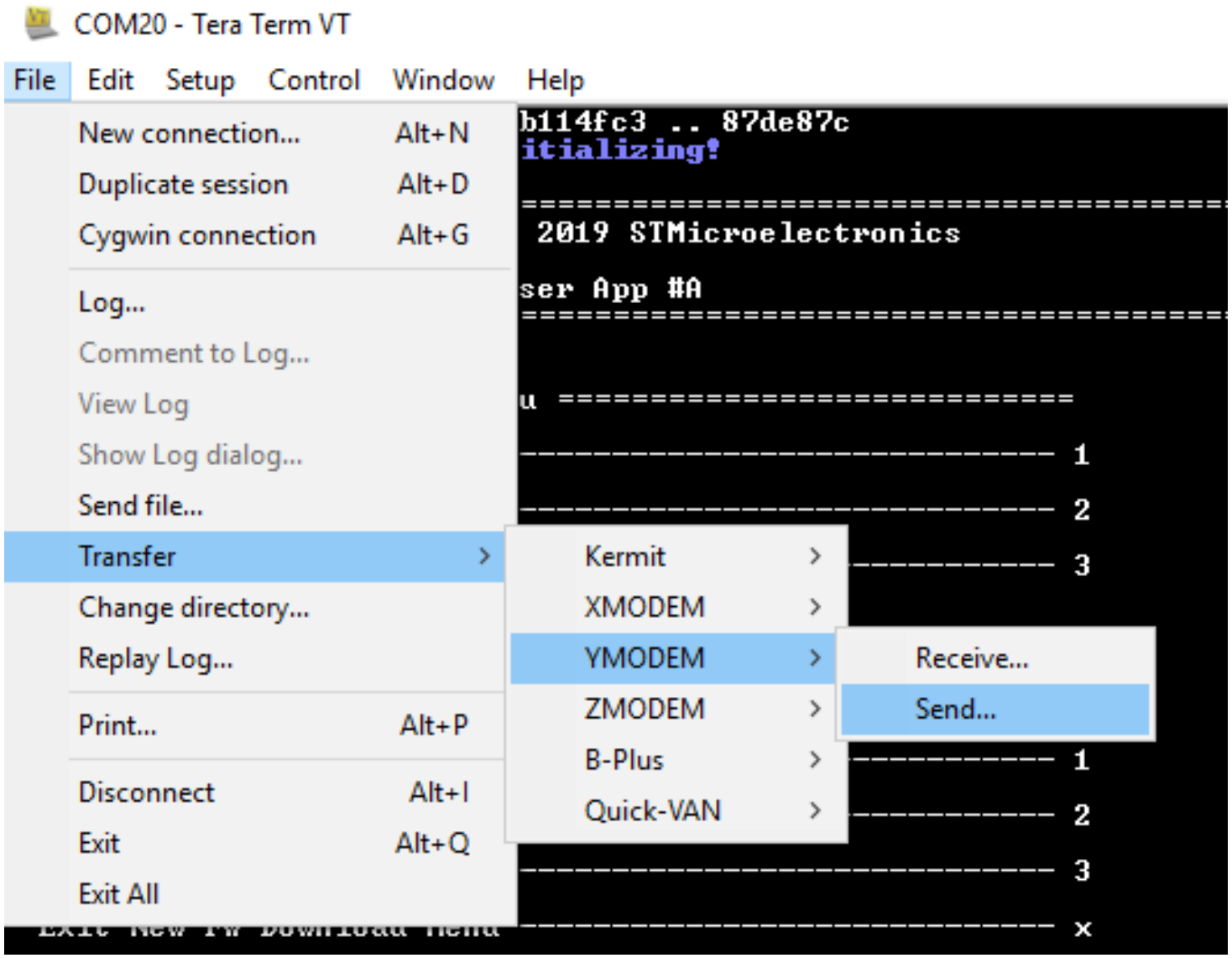
```
=================================================================
=              (C) COPYRIGHT 2019 STMicroelectronics            =
=                                                               =
=                          User App #A                          =
=================================================================

=================== Main Menu ============================

  Test Protections ------------------------------------- 1

  Test TFM --------------------------------------------- 2

  Download a new Fw Image ------------------------------ 3

  Selection :

================ New Fw Download =========================

  Reset to trigger Installation ------------------------- 1

  Download Secure Image --------------------------------- 2

  Download NonSecure Image ------------------------------ 3

  Exit New FW Download Menu ----------------------------- x
```

```
=================================================================
=              (C) COPYRIGHT 2019 STMicroelectronics            =
=                                                               =
=                          User App #A                          =
=================================================================

=================== Main Menu ============================

  Test Protections ------------------------------------- 1

  Test TFM --------------------------------------------- 2

  Download a new Fw Image ------------------------------ 3

  Selection :

================ New Fw Download =========================

  Reset to trigger Installation ------------------------- 1

  Download Secure Image --------------------------------- 2

  Download NonSecure Image ------------------------------ 3

  Exit New FW Download Menu ----------------------------- x

Download Secure Image
  -- Send Firmware

  -- -- File> Transfer> YMODEM> Send
```

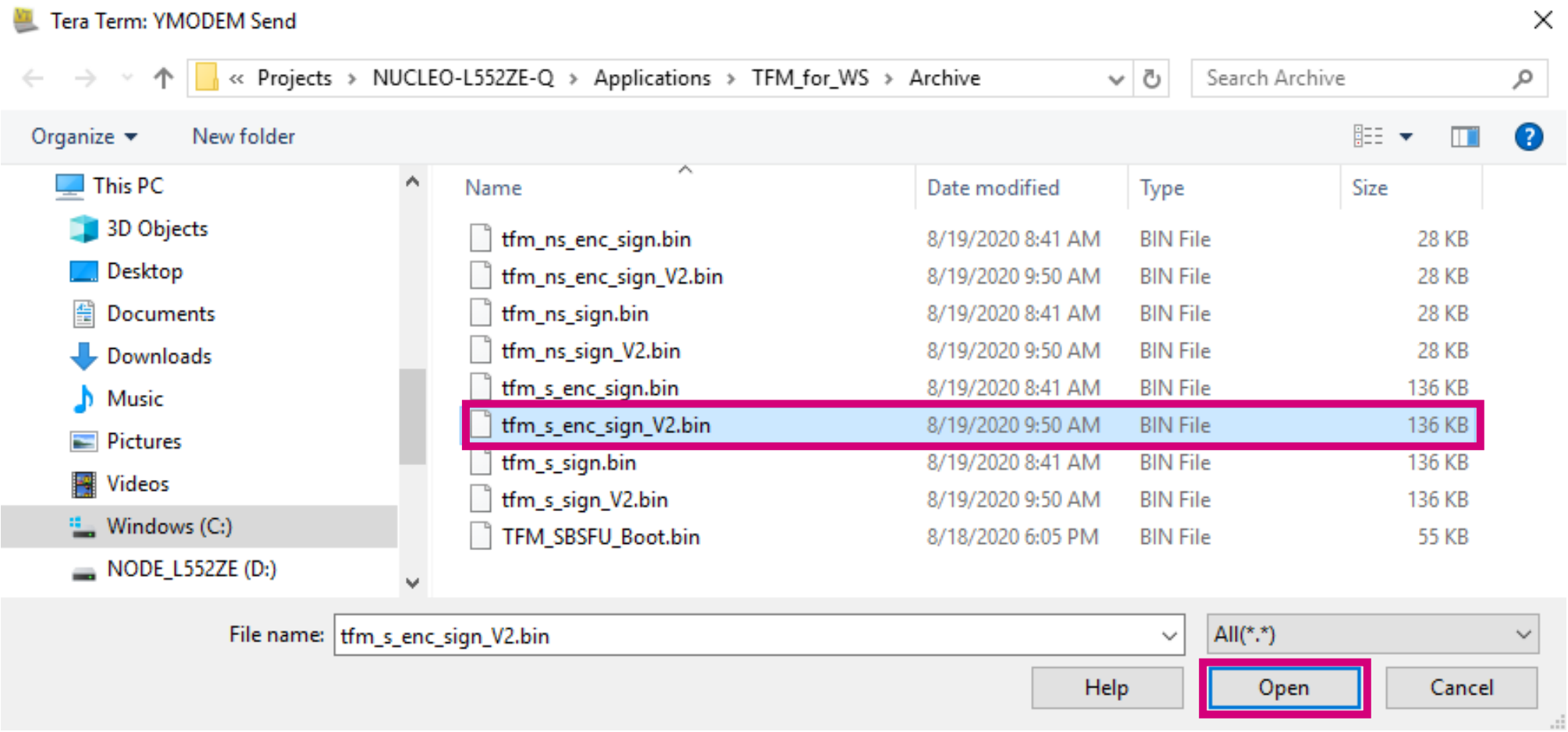
- Select Download Secure Image

life.augmented

Download new secure firmware menu



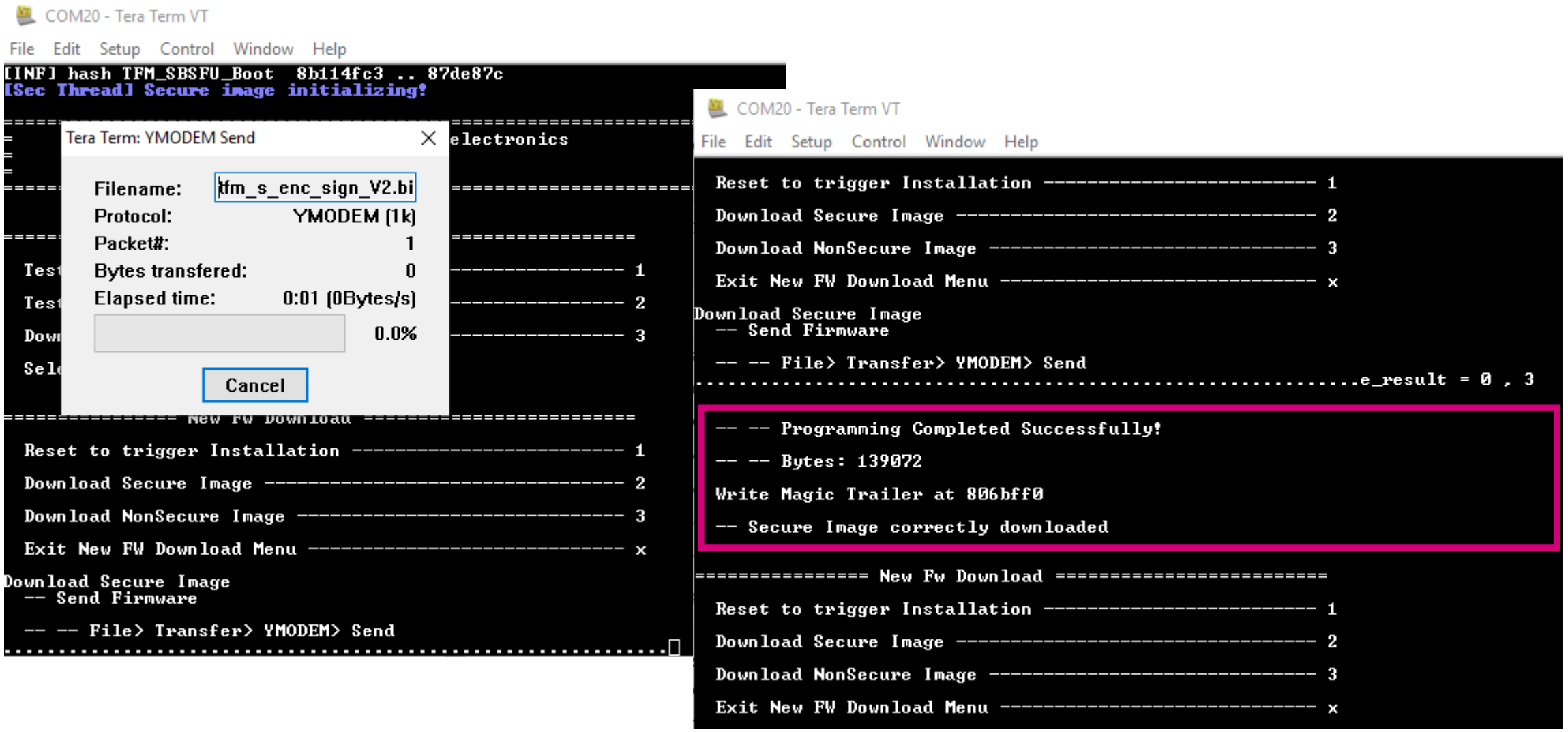
Download new secure firmware menu



- If you want to use the non-encrypted version select : tfm_s_sign_V2.bin

life.augmented

Download new secure firmware menu



- Then reset to trigger installation (press 1 or Reset Button)

Download new secure firmware menu

```
  -- Install image : reboot

[INF] Starting bootloader
[INF] Checking BL2 NV area
[INF] Checking BL2 NV area header
[INF] Checking BL2 NV Counter consitency
[INF] Consistent BL2 NV Counter 3   = 0x1000000
[INF] Consistent BL2 NV Counter 4   = 0x1000000
[INF] Swap type: test
[INF] d, 70, 93, d4, f2, 3c , 24 ,a3,
[INF] 9a, 6, 97, 89, 86, 2f , d ,58,
[INF] verify counter  0 2000000 1000000
[INF] counter  0 : ok
[INF] verify sig key id 0
[INF] signature OK
[INF] swap type: none
[INF] Image upgrade secondary slot -> primary slot
[INF] Erasing the primary slot
[INF] d, 70, 93, d4, f2, 3c , 24 ,a3,
[INF] 9a, 6, 97, 89, 86, 2f , d ,58,
[INF] Copying the secondary slot to the primary slot: 0x24000 bytes
[INF] Counter 3 set to 0x2000000
[INF] verify counter  0 2000000 2000000
[INF] counter  0 : ok
[INF] verify sig key id 0
[INF] signature OK
[INF] verify counter  1 1000000 1000000
[INF] counter  1 : ok
[INF] verify sig key id 1
[INF] signature OK
[INF] Bootloader chainload address offset: 0x14000
[INF] Jumping to the first image slot
[INF] BL2 HUK _STM32L652XX_HUK_CUSTOMIZATION_
 set to BL2 SHARED DATA
[INF] Code c001900 c00ea7a
[INF] back TFM_SPSEL_Reset  9b114fe3    87de87e
[Sec Thread] This is a version 2 prepared for Security Workshop...
[Sec Thread] Secure image initializing!

==================================================================
=              (C) COPYRIGHT 2019 STMicroelectronics             =
=                                                                =
=                          User App #A                           =
==================================================================
```

Current version counter for secure and non secure

There is an image in slot 2, we will test before swap

Check of new version and signature

Image update
Update of the counter

New version of secure app is executed

life.augmented

Download nonsecure firmware menu

COM20 - Tera Term VT

File Edit Setup Control Window Help

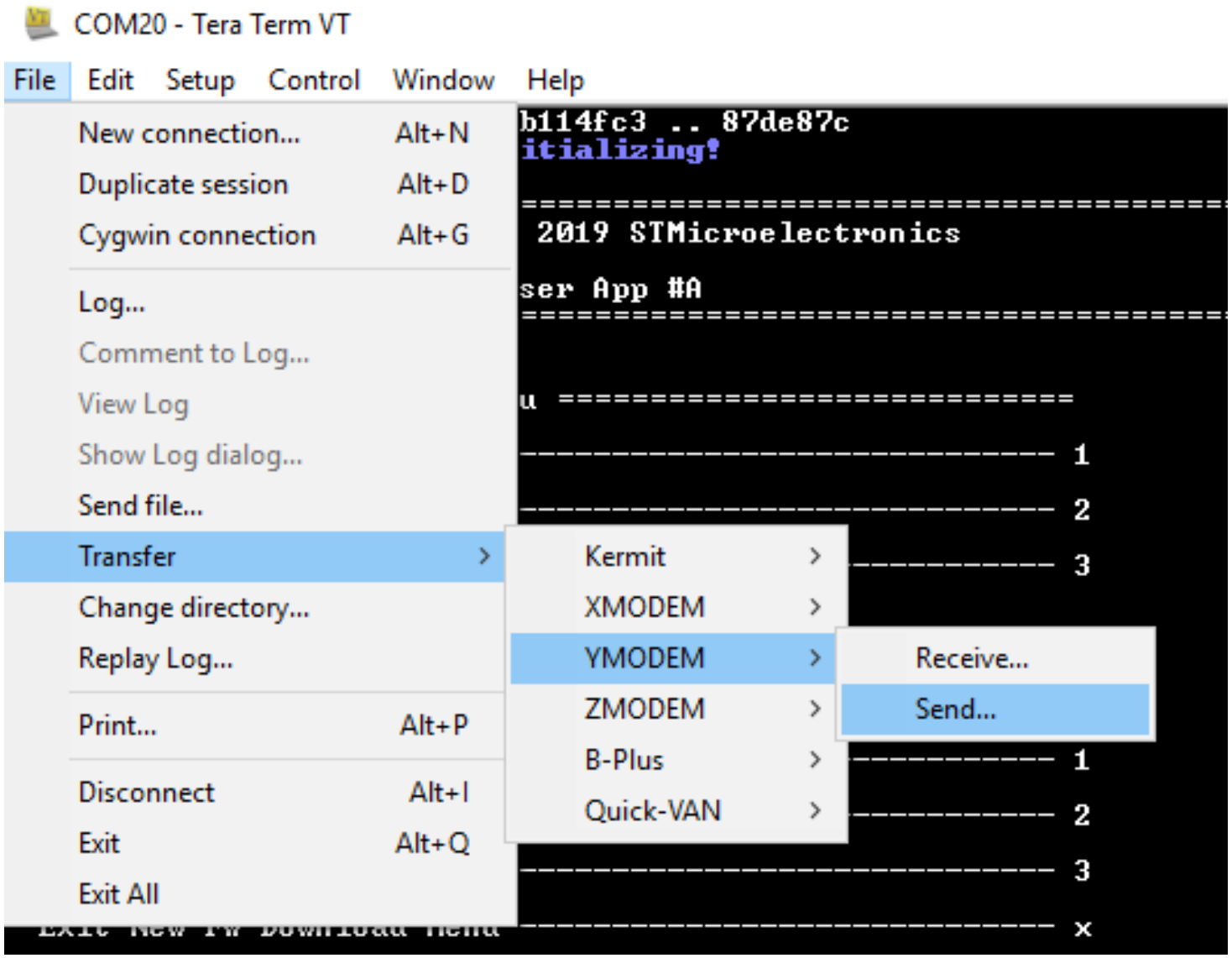
```
==============================================================================
=              (C) COPYRIGHT 2019 STMicroelectronics                         =
=                                                                            =
=                          User App #A                                       =
==============================================================================

=================== Main Menu ============================
  Test Protections ------------------------------------- 1
  Test TFM --------------------------------------------- 2
  Download a new Fw Image ------------------------------ 3
  Selection :

================ New Fw Download =========================
  Reset to trigger Installation ------------------------- 1
  Download Secure Image --------------------------------- 2
  Download NonSecure Image ------------------------------ 3
  Exit New FW Download Menu ----------------------------- x
```

```
==============================================================================
=              (C) COPYRIGHT 2019 STMicroelectronics                         =
=                                                                            =
=                          User App #A                                       =
==============================================================================

=================== Main Menu ============================
  Test Protections ------------------------------------- 1
  Test TFM --------------------------------------------- 2
  Download a new Fw Image ------------------------------ 3
  Selection :

================ New Fw Download =========================
  Reset to trigger Installation ------------------------- 1
  Download Secure Image --------------------------------- 2
  Download NonSecure Image ------------------------------ 3
  Exit New FW Download Menu ----------------------------- x
Download NonSecure Image
  -- Send Firmware

  -- -- File> Transfer> YMODEM> Send
..
```

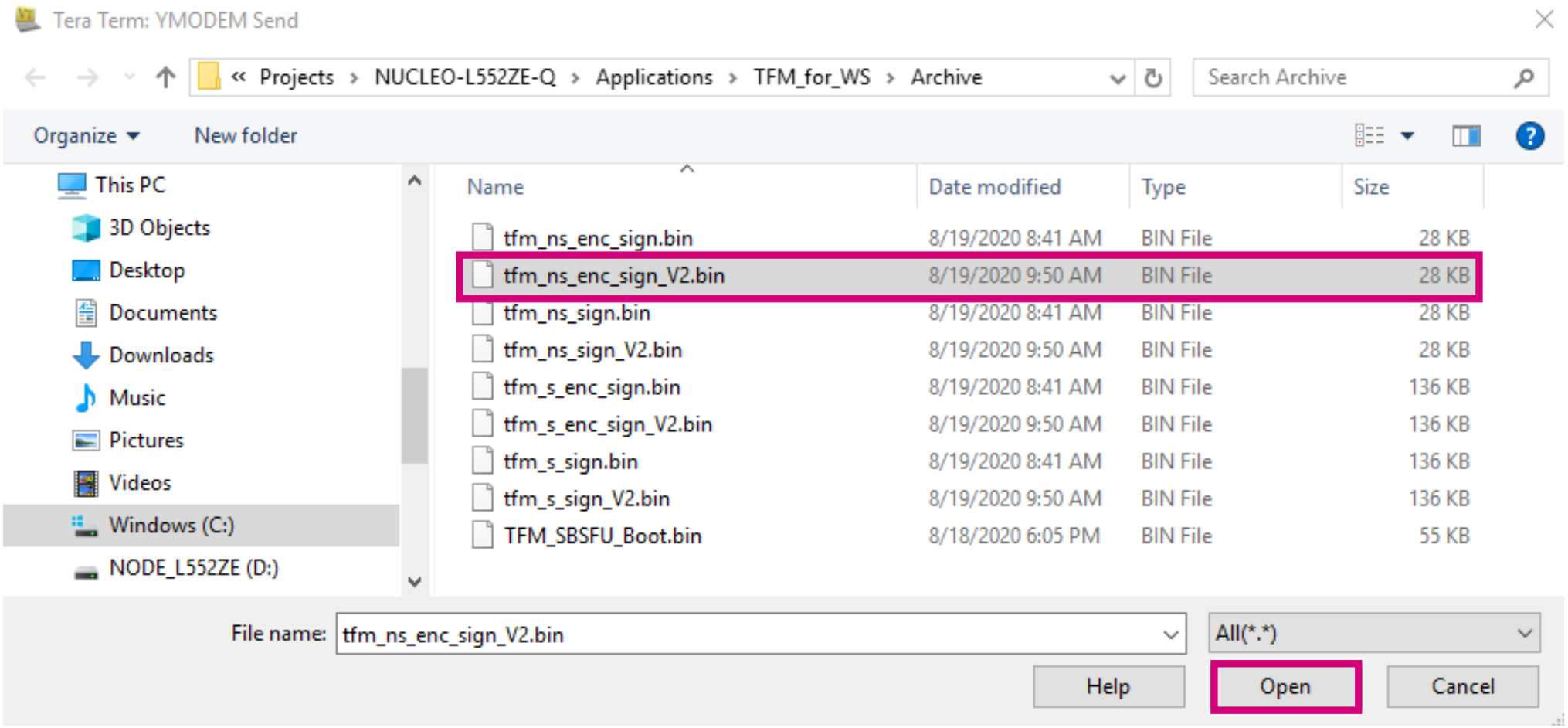
- Select Download Nonsecure Image

life.augmented

Download nonsecure firmware menu

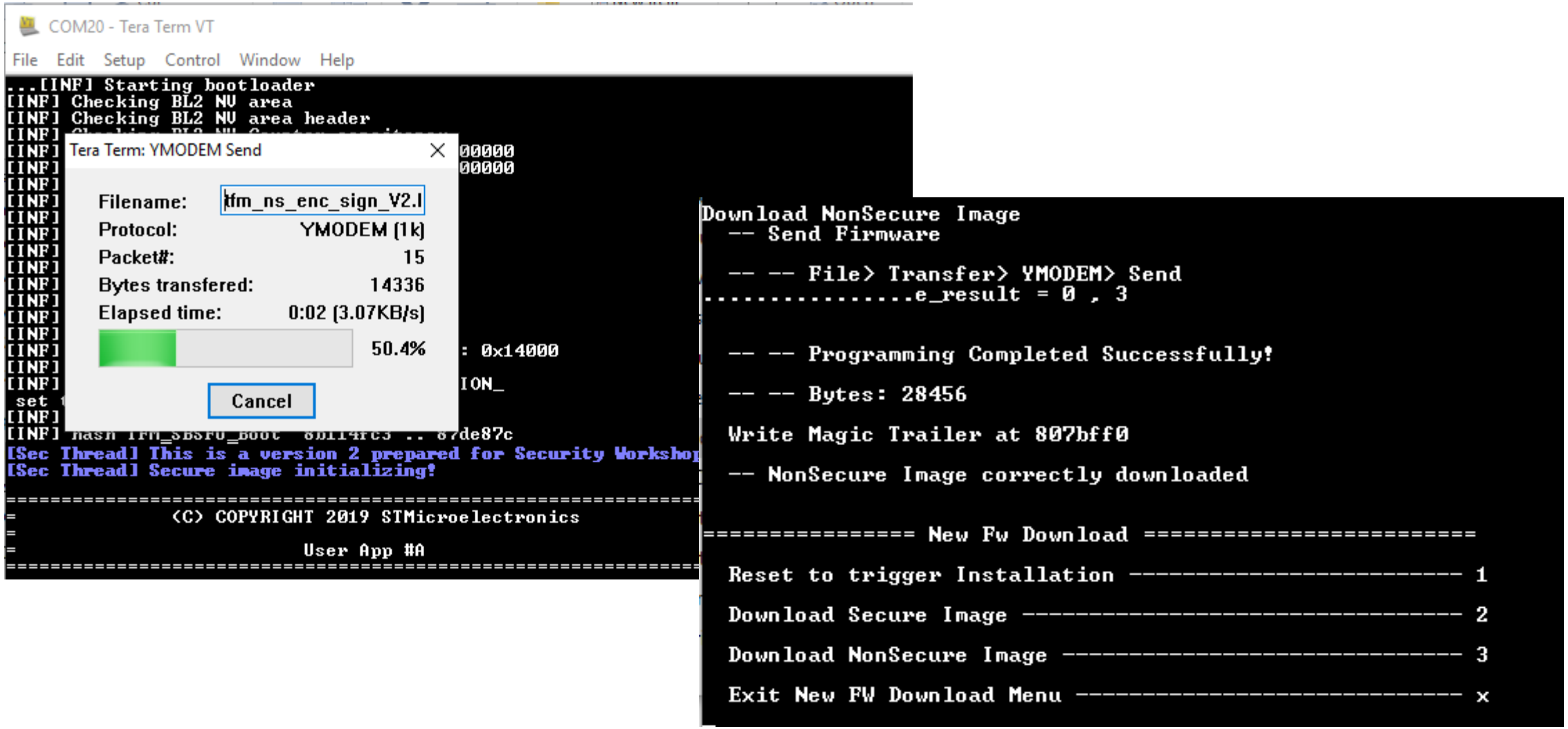


Download nonsecure firmware menu



- If you want to use the non-encrypted version select : tfm_ns_sign_V2.bin

Download nonsecure firmware menu



- Then reset to trigger installation (press 1 or Reset Button)

Download nonsecure firmware menu

```
  -- Install image : reboot

[INF] Starting bootloader
[INF] Checking BL2 NV area
[INF] Checking BL2 NV area header
[INF] Checking BL2 NV Counter consitency
[INF] Consistent BL2 NV Counter 3  = 0x2000000
[INF] Consistent BL2 NV Counter 4  = 0x1000000
[INF] Swap type: none
[INF] Swap type: test
[INF] b5, b9, 95, b1, 75, 24 , 2a ,78,
[INF] 29, 2b, 99, 9, 9, fb , a9 ,e0,
[INF] verify counter  1 2000000 1000000
[INF] counter  1 : ok
[INF] verify sig key id 1
[INF] signature OK
[INF] Image upgrade secondary slot -> primary slot
[INF] Erasing the primary slot
[INF] b5, b9, 95, b1, 75, 24 , 2a ,78,
[INF] 29, 2b, 99, 9, 9, fb , a9 ,e0,
[INF] Copying the secondary slot to the primary slot: 0x10000 bytes
[INF] Counter 4 set to 0x2000000
[INF] verify counter  0 2000000 2000000
[INF] counter  0 : ok
[INF] verify sig key id 0
[INF] signature OK
[INF] verify counter  1 2000000 2000000
[INF] counter  1 : ok
[INF] verify sig key id 1
[INF] signature OK
[INF] Bootloader chainload address offset: 0x14000
[INF] Jumping to the first image slot
[INF] BL2 HUK _STM32L652XX_HUK_CUSTOMIZATION_
 set to BL2 SHARED DATA
[INF] Code c001900 c00ea7a
[INF] hash TFM_SBSFU_Boot  8b114fc3 .. 87de87c
[Sec Thread] This is a version 2 prepared for Security Workshop...
[Sec Thread] Secure image initializing!

==================================================================
=              (C) COPYRIGHT 2019 STMicroelectronics             =
=                                                                =
=                          User App #B                           =
==================================================================
```

Current version counter for secure and non secure

There is an image in slot 2, we will test before swap

Check of new version and signature

Image update
Update of the counter

New version of non-secure app is executed

life.augmented

Test Protection menu

```
==================================================================
=              (C) COPYRIGHT 2019 STMicroelectronics             =
=                                                                =
=                          User App #B                           =
==================================================================

==================== Main Menu ============================
 Test Protections ------------------------------------- 1
 Test TFM --------------------------------------------- 2
 Download a new Fw Image ------------------------------ 3
 Selection :

==================== Test Menu ============================
 Test Protection : NonSecure try to access to Secure --- 1
 RDP Regression --------------------------------------- 2
 Previous Menu ---------------------------------------- x
```

- Test access from non-secure to secure domain (SRAM/Flash/RNG and BACKUP register)

life.augmented

Test Protection result

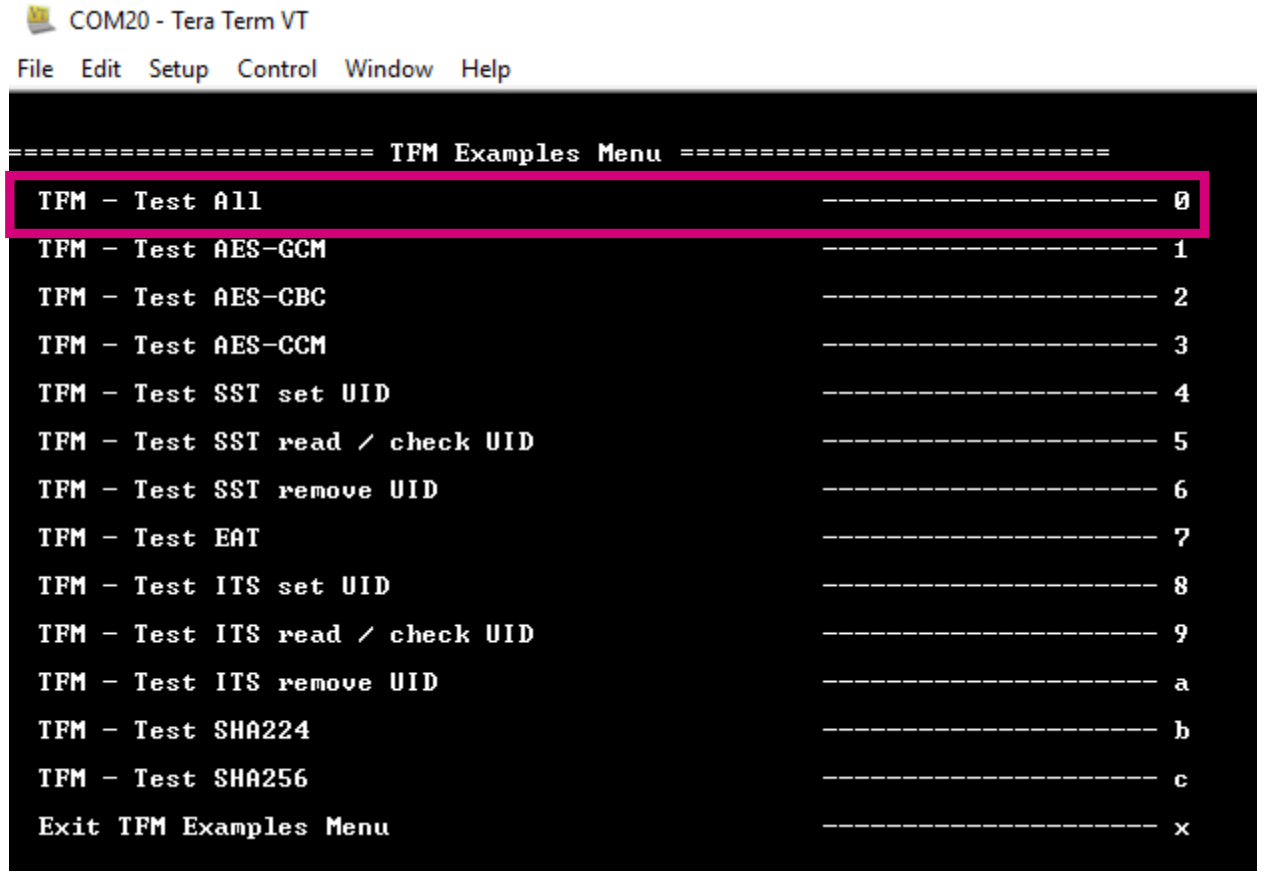
```
= [TEST] read 1 byte @ Code Secure END(veneer) 0c038400[Sec Handler] Oops... Secure fault!!! You're no
t going anywhere!
[INF] Starting bootloader
[INF] Checking BL2 NV area
[INF] Checking BL2 NV area header
[INF] Checking BL2 NV Counter consitency
[INF] Consistent BL2 NV Counter 3  = 0x2000000
[INF] Consistent BL2 NV Counter 4  = 0x2000000
[INF] Swap type: none
[INF] Swap type: none
[INF] verify counter  0 2000000 2000000
[INF] counter  0 : ok
[INF] verify sig key id 0
[INF] signature OK
[INF] verify counter  1 2000000 2000000
[INF] counter  1 : ok
[INF] verify sig key id 1
[INF] signature OK
[INF] Bootloader chainload address offset: 0x14000
[INF] Jumping to the first image slot
[INF] BL2 HUK _STM32L652XX_HUK_CUSTOMIZATION_
 set to BL2 SHARED DATA
[INF] Code c001900 c00ea7a
[INF] hash TFM_SBSFU_Boot  8b114fc3 .. 87de87c
[Sec Thread] This is a version 2 prepared for Security Workshop...
[Sec Thread] Secure image initializing!

= [TEST] read 4 bytes @ RNG IP SR 420c0804
= [TEST] read 4 bytes @ RNG IP DR 420c0808
= [TEST] read 4 bytes @ BACKUP REG 0 40003500
= [TEST] read 4 bytes @ BACKUP REG 7 4000351c
 TEST_PROTECTIONS_Run_SecUserMem : Passed
```

Test TFM menu

```
=================================================================
=              (C) COPYRIGHT 2019 STMicroelectronics            =
=                                                               =
=                          User App #B                          =
=================================================================


=================== Main Menu ============================

  Test Protections ------------------------------------- 1

  Test TFM --------------------------------------------- 2

  Download a new Fw Image ------------------------------- 3

  Selection :
```

life.augmented

Test TFM menu



- This allow you to launch test of secure service of TFM

life.augmented

Test TFM Result

COM20 - Tera Term VT

File Edit Setup Control Window Help

```
AES GCM test SUCCESSFULL
AES CBC test SUCCESSFULL
AES CCM test SUCCESSFULL
SST set UID test SUCCESSFULL
SST read / check UID test SUCCESSFULL
SST remove UID test SUCCESSFULL
token request value :
00000000000000000000000000000000000000000
00000000000000000000000000000000000000000
00000000000000000000000000000000000000000
00000000

token response value :
d28443a10126a0590193a83a000124ff58400000
00000000000000000000000000000000000000000
00000000000000000000000000000000000000000
00000000000000000000000000000000000000000
00003a000124fb5820053fe7b397872018b24e07
8cee9d2dd25e25c1f16b613fc6d12bad0e0582b3
fc3a00012500582101fa58755f658627ce5460f2
9b75296713248cae7ad9e2984b90280efcbcb502
483a000124fa58208b114fc398f8e2183451508d
4e987758e38d571bd3a2899b4e8ea965870de87c
3a000124f8203a000124f91930003a000124fd82
a501635350450465322e302e30025820930f2d69
ab3eb718c6c27448d8b2f75e761d2e2f4755e188
d9cc21b231f321f1066653484132353605582 0fc
5701dc6135e1323847bdc40f04d2e5bee5833b23
c29f93593d00018cfa9994a501644e5350450465
322e302e3002582077b58f309fdbc442aa2ae716
4c7989bf1b10e3a863643571e2049e2ca67db319
0666534841323536055820e18015993d6d2760b4
99274baef264b83af229e9a785f3d5bf00b9d32c
1f03963a000124fc64726400205840d21667871e
59772fc934aa73ed71532083d9b628a0ccb60ae7
a8542fd0fc047f417012371bde43bf7f6de19196
e926cc8b19f13df7db7d165d7d7f18a66b8ae3

EAT normal circuit sig test SUCCESSFULL
ITS set UID test SUCCESSFULL
ITS read / check UID test SUCCESSFULL
ITS remove UID test SUCCESSFULL
SHA224 test SUCCESSFULL
SHA256 test SUCCESSFULL
CUMULATIVE RESULT: 12/12 success

======================= TFM Examples Menu ==========================
```

life.augmented

Where do we stand?

- So we experiment TFM-SBSFU functionalities:
  - Update TFM Appli Secure
  - Update TFM Appli NonSecure
  - Test some security service call thanks test embedded in the user app
- Next possible hands-On
  - Compile and debug TFM_SBSFU_Boot / TFM Appli Secure / TFM Appli NonSecure
  - Activate HDP
  - Activate RDP 0.5
- If you stop here, please go to slide “Board clean up!” (at the end of this presentation)

Compile and debug TFM

First clean up the board…

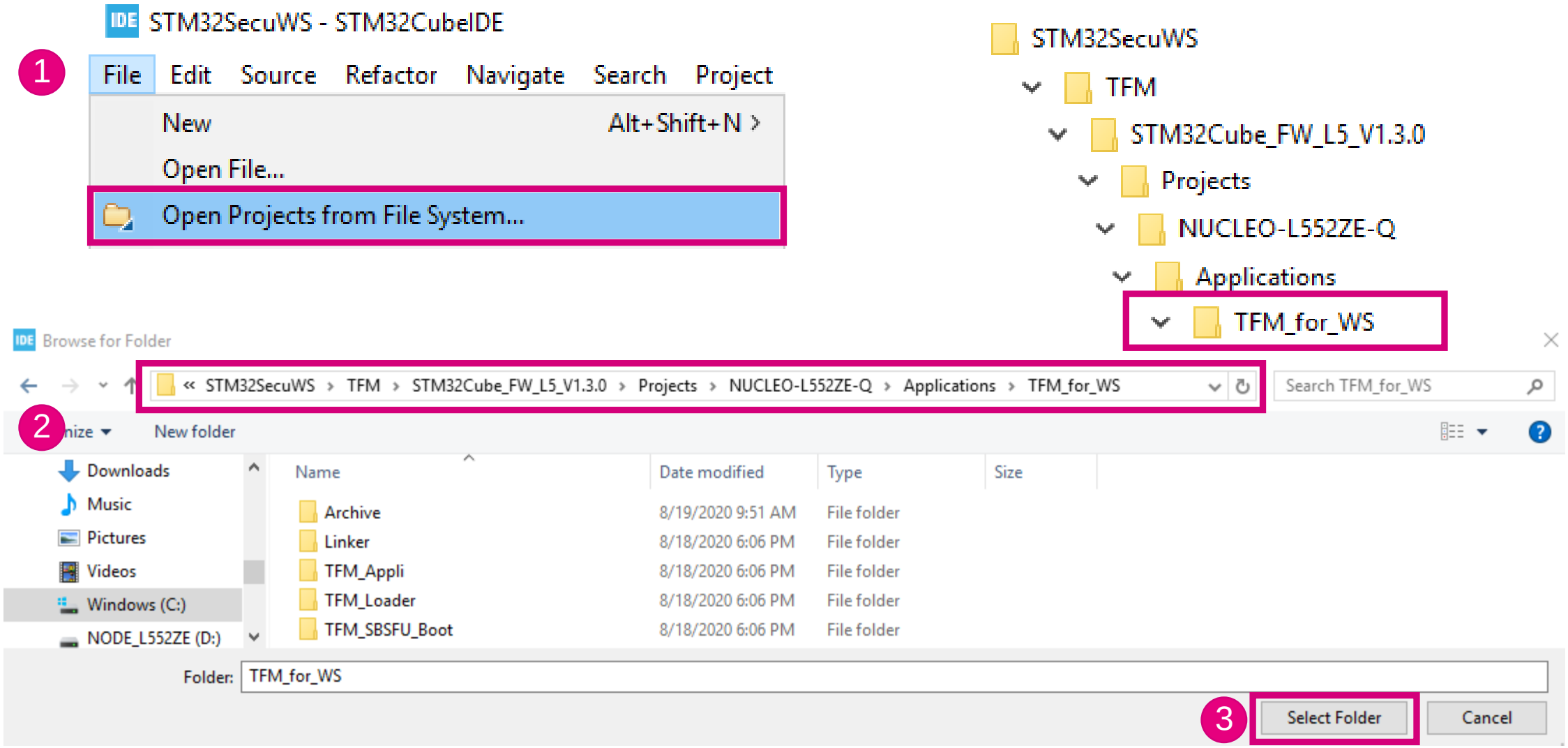
C:\STM32SecuWS\TFM\Scripts

- Please launch :
  - STEP3_flash_mass_erase.bat

C:\windows\system32\cmd.exe

```
C:\STM32SecuWS\TFM\Scripts>echo OFF
"TFM_Appli NonSecure started"
      -------------------------------------------------------------------
                        STM32CubeProgrammer v2.5.0
      -------------------------------------------------------------------

ST-LINK SN  : 066FFF505352716587230728
ST-LINK FW  : V2J37M26
Board       : NUCLEO-L552ZE-Q
Voltage     : 3.25V
SWD freq    : 4000 KHz
Connect mode: Hot Plug
Reset mode  : Software reset
Device ID   : 0x472
Revision ID : Rev B
Device name : STM32L5xx
Flash size  : 512 KBytes
Device type : MCU
Device CPU  : Cortex-M33


Mass erase ...

Mass erase successfully achieved

MCU Reset

Software reset is performed
"Mass erase done, press a key"
Press any key to continue . . .
```

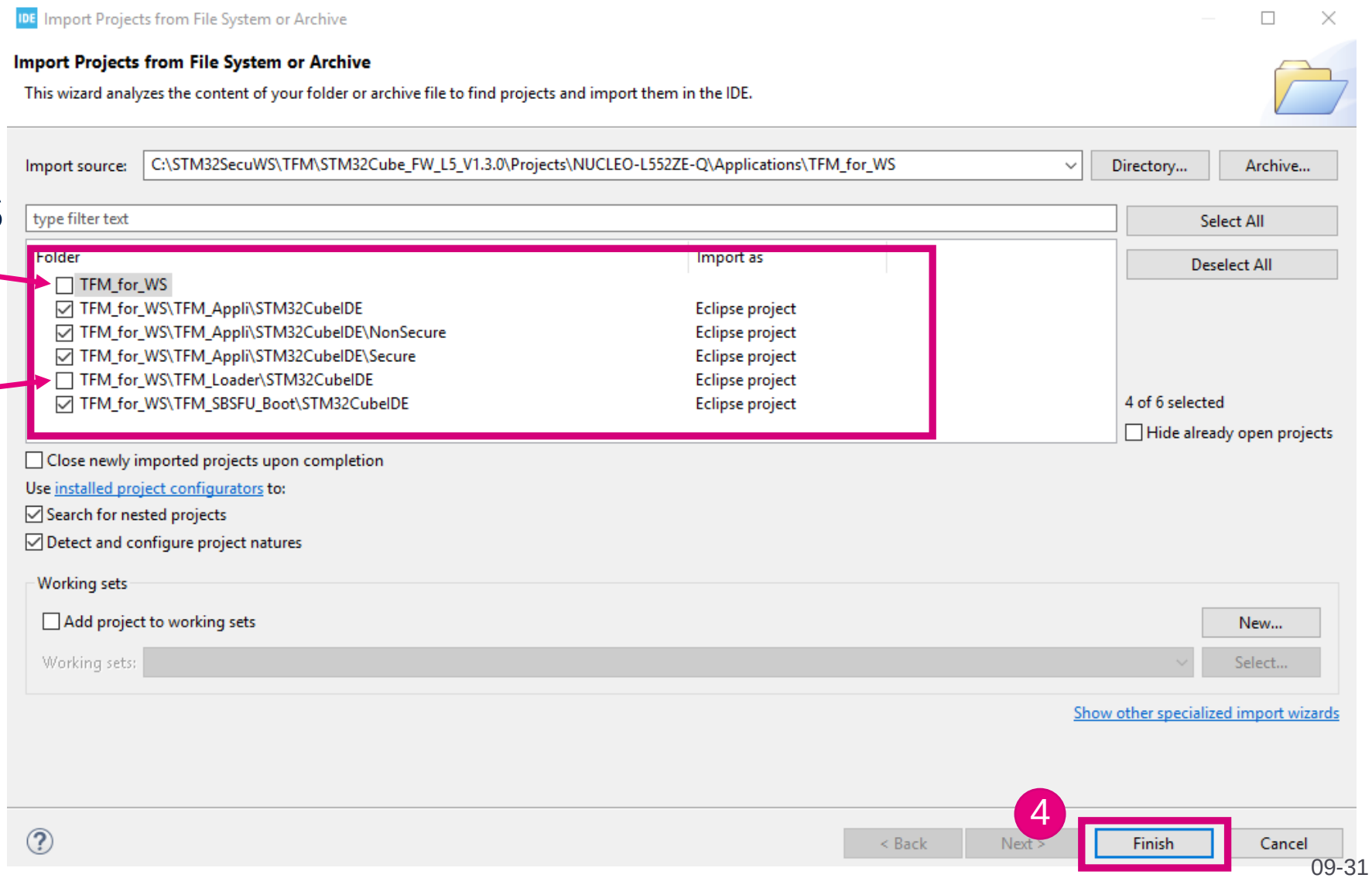
Compile the TFM software



Compile the TFM software

2 Uncheck TFM_for_WS

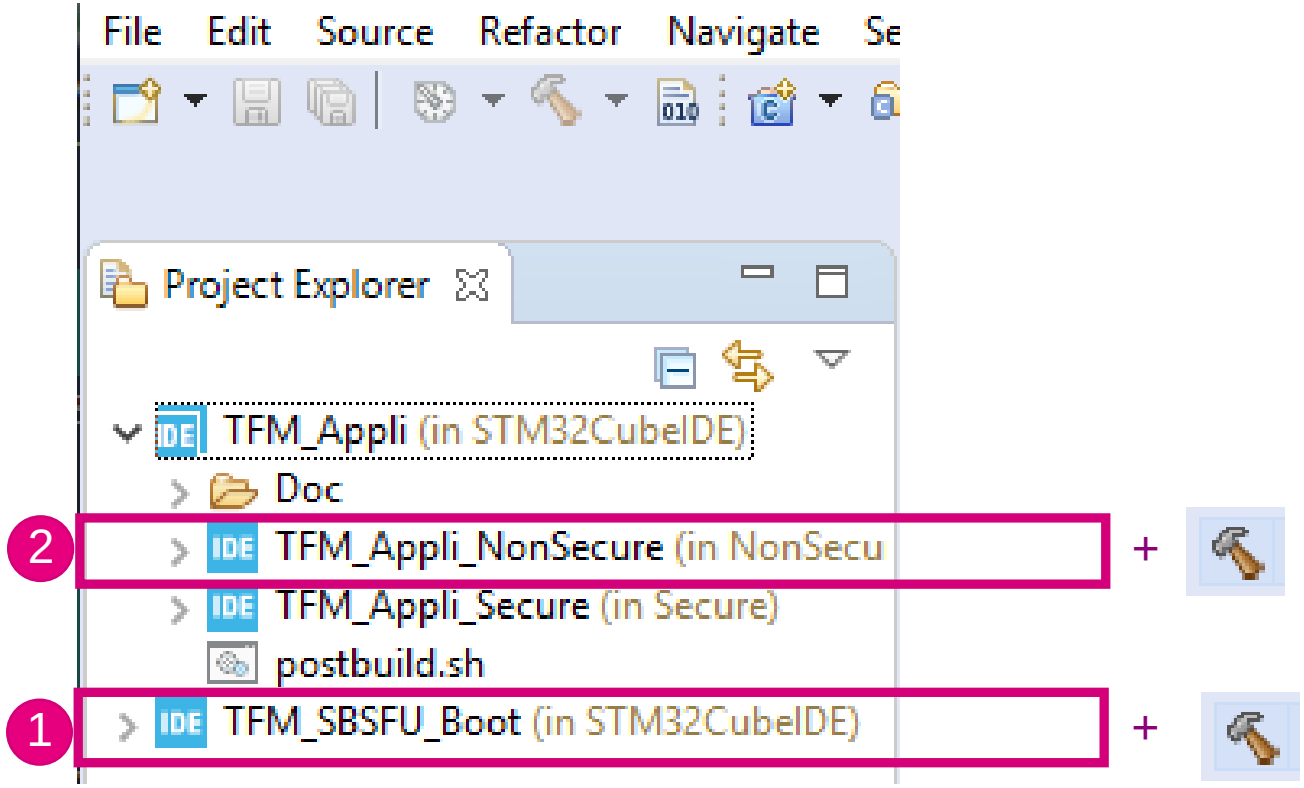
3 Uncheck TFM_Loader



life.augmented

Compile the TFM software

- Compile in this order (click on the project + CTRL B or )
  - TFM_SBSFU_Boot
  - TFM_Appli_NonSecure



Compile the TFM software

Problems | Tasks | Console | Properties

CDT Build Console [TFM_SBSFU_Boot]

```
   text    data     bss     dec     hex filename
  48936     320   56320  105576   19c68 TFM_SBSFU_Boot.elf
Finished building: default.size.stdout

Finished building: TFM_SBSFU_Boot.bin

Finished building: TFM_SBSFU_Boot.list

arm-none-eabi-objcopy -O binary "TFM_SBSFU_Boot.elf" "TFM_SBSFU_Boot.bin"
arm-none-eabi-size "TFM_SBSFU_Boot.elf"
   text    data     bss     dec     hex filename
  48936     320   56320  105576   19c68 TFM_SBSFU_Boot.elf
arm-none-eabi-objdump -DS  "TFM_SBSFU_Boot.elf" > "TFM_SBSFU_Boot.elf_asm.txt"
"../postbuild.sh"
C:/STM32SecuWS/TFM/STM32Cube_FW_L5_V1.3.0/Projects/NUCLEO-L552ZE-Q/Applications
Windows_NT
Postbuild with windows executable
 updated
C:/STM32SecuWS/TFM/STM32Cube_FW_L5_V1.3.0/Projects/NUCLEO-L552ZE-Q/Applications
C:/STM32SecuWS/TFM/STM32Cube_FW_L5_V1.3.0/Projects/NUCLEO-L552ZE-Q/Applications

11:41:19 Build Finished. 0 errors, 0 warnings. (took 55s.68ms)
```

1

Problems | Tasks | Console | Properties

CDT Build Console [TFM_Appli_Secure]

```
Finished building: TFM_Appli_Secure.bin

Finished building: TFM_Appli_Secure.list

arm-none-eabi-objcopy -O binary "TFM_Appli_Secure.elf" "TFM_Appli_Secure.bin"
"../../postbuild.sh" "."  "1.0.0+0" "secure"
C:/STM32SecuWS/TFM/STM32Cube_FW_L5_V1.3.0/Projects/NUCLEO-L552ZE-Q/Applications/
Windows_NT
Postbuild with windows executable
secure rsa2048  image_number=2
secure signing
secure encrypting


12:56:08 Build Finished. 0 errors, 0 warnings. (took 1m:5s.325ms)
```

2

CDT Build Console [TFM_Appli_NonSecure]

```
Finished building: TFM_Appli_NonSecure.bin

Finished building: TFM_Appli_NonSecure.list

arm-none-eabi-objcopy -O binary "TFM_Appli_NonSecure.elf" "TFM_Appli_NonSecure.bin"
"../../postbuild.sh" "."  "1.0.0+0" "nonsecure"
C:/STM32SecuWS/TFM/STM32Cube_FW_L5_V1.3.0/Projects/NUCLEO-L552ZE-Q/Applications/TFM_
Windows_NT
Postbuild with windows executable
nonsecure rsa2048  image_number=2
nonsecure signing
nonsecure encrypting


12:56:25 Build Finished. 0 errors, 0 warnings. (took 15s.720ms)
```

3

life.augmented

Questions

- Question : Could I use CubeIDE to flash the generated binaries ?
- Answer :
  It is possible for TFM-SBSFU but not for TFM-Appli_Secure and TFM-Appli_NonSecure from a functional point of view…
- Question Why ?
- Answer :
  TFM-Appli_Secure and TFM-Appli_NonSecure are signed, so we won't flash directly the binary generated but the signed binary available in this folder C:\STM32SecuWS\TFM\STM32Cube_FW_L5_V1.3.0\Projects\NUCLEO-L552ZE-Q\Applications\TFM_for_WS\TFM_Appli\Binary

Flash the TFM software

C:\STM32SecuWS\TFM\Scripts

- Please launch in this order :
  - STEP4_flash_ns_binary.bat
  - STEP5_flash_s_binary.bat
  - STEP6_flash_SBSFU_binary.bat
- For each script please have a look in the trace to insure there is no issue
- If not done or you closed the window, launch TeraTerm :
  - StartTeraTermL5.bat

life.augmented

Flash the TFM software

C:\windows\system32\cmd.exe

```
Memory Programming ...
Opening and parsing file: tfm_ns_sign.bin
  File          : tfm_ns_sign.bin
  Size          : 28196 Bytes
  Address       : 0x08038000

Erasing memory corresponding to segment 0:
Erasing internal memory sectors [112 125]
Download in Progress:

File download complete
Time elapsed during download operation: 00

Verifying ...

Read progress:

Download verified successfully

"TFM_Appli NonSecure Written, press a key"
Press any key to continue . . .
```

C:\windows\system32\cmd.exe

```
Memory Programming ...
Opening and parsing file: tfm_s_sign.bin
  File          : tfm_s_sign.bin
  Size          : 138812 Bytes
  Address       : 0x0C014000

Erasing memory corresponding to segment 0
Erasing internal memory sectors [40 107]
Download in Progress:

File download complete
Time elapsed during download operation: 0

Verifying ...

Read progress:

Download verified successfully

"TFM_Appli Secure Written, press a key"
Press any key to continue . . .
```

C:\windows\system32\cmd.exe

```
Memory Programming ...
Opening and parsing file: TFM_SBSFU_Boot.bin
  File          : TFM_SBSFU_Boot.bin
  Size          : 55930 Bytes
  Address       : 0x0C001000

Erasing memory corresponding to segment 0:
Erasing internal memory sectors [2 29]
Download in Progress:
                                                  100%
File download complete
Time elapsed during download operation: 00:00:02.152

Verifying ...

Read progress:
                                                  100%
Download verified successfully

"TFM SBSFU Done, press a key"
Press any key to continue . . .
```

life.augmented

Flash the TFM software

- Check with Teraterm

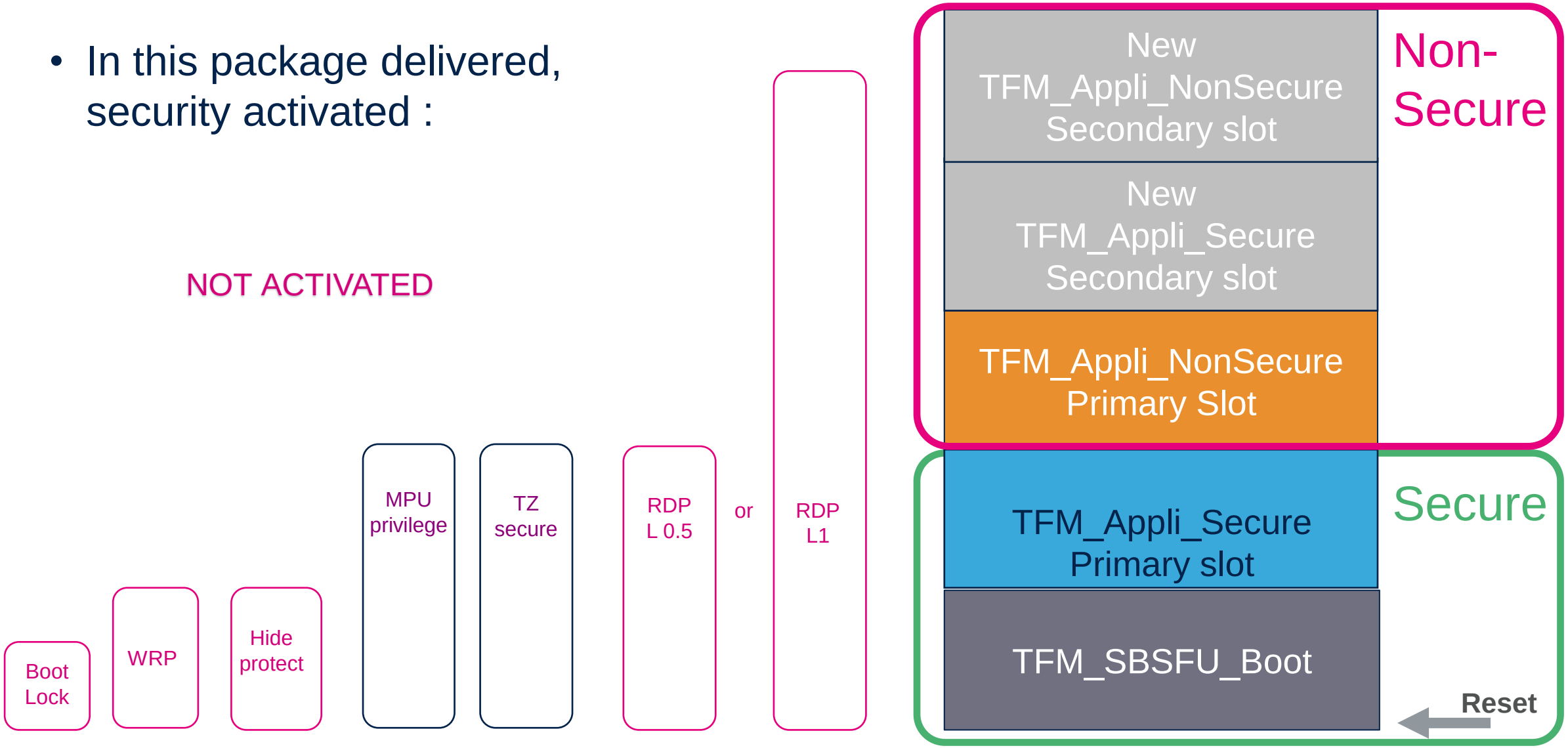
COM20 - Tera Term VT

File Edit Setup Control Window Help

```
[INF] Starting bootloader
[INF] Initializing BL2 NV area : Power down/reset not supported...
[INF] Init BL2 NV Header area: Done
[INF] Initializing BL2 NV Counters
[INF] Init BL2 NV counters to 0 : Done
[INF] BL2 NV Area Initialized : Power Down/reset supported
[INF] Checking BL2 NV area
[INF] Checking BL2 NV area header
[INF] Checking BL2 NV Counter consitency
[INF] Consistent BL2 NV Counter 3  = 0x0
[INF] Consistent BL2 NV Counter 4  = 0x0
[INF] Swap type: none
[INF] Swap type: none
[INF] verify counter  0 1000000 0
[INF] counter  0 : ok
[INF] verify sig key id 0
[INF] signature OK
[INF] Counter 3 set to 0x1000000
[INF] verify counter  1 1000000 0
[INF] counter  1 : ok
[INF] verify sig key id 1
[INF] signature OK
[INF] Counter 4 set to 0x1000000
[INF] Bootloader chainload address offset: 0x14000
[INF] Jumping to the first image slot
[INF] BL2 HUK _STM32L652XX_HUK_CUSTOMIZATION_
 set to BL2 SHARED DATA
[INF] Code c001900 c00ea7a
[INF] hash TFM_SBSFU_Boot  8b114fc3 .. 87de87c
[Sec Thread] Secure image initializing!

=====================================================================
=              (C) COPYRIGHT 2019 STMicroelectronics                =
=                                                                   =
=                          User App #A                              =
=====================================================================


=================== Main Menu ============================

  Test Protections ---------------------------------------- 1

  Test TFM ------------------------------------------------ 2

  Download a new Fw Image -------------------------------- 3

  Selection :
```

Which security are activated ?

- In this package delivered, security activated :

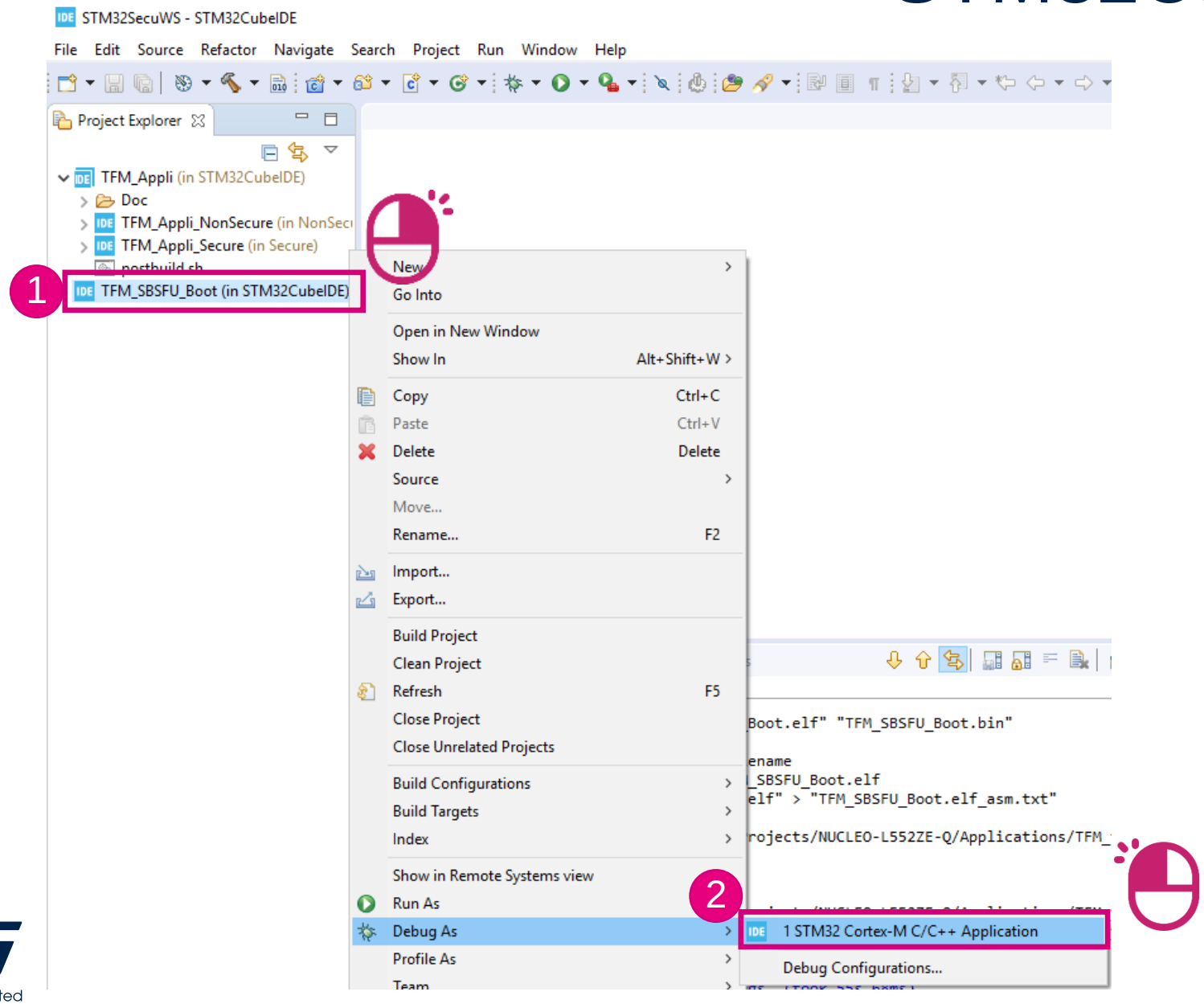


STM32CubeIDE debugging

- Let’s debug TFM !
  - Create a new debug config based on the TFM_SBSFU_Boot config
  - Remove the download from the debug configuration of the TFM_SBSFU_Boot
  - Add the loading of the TFM_Appli_Secure and TFM_Appli_NonSecure symbol

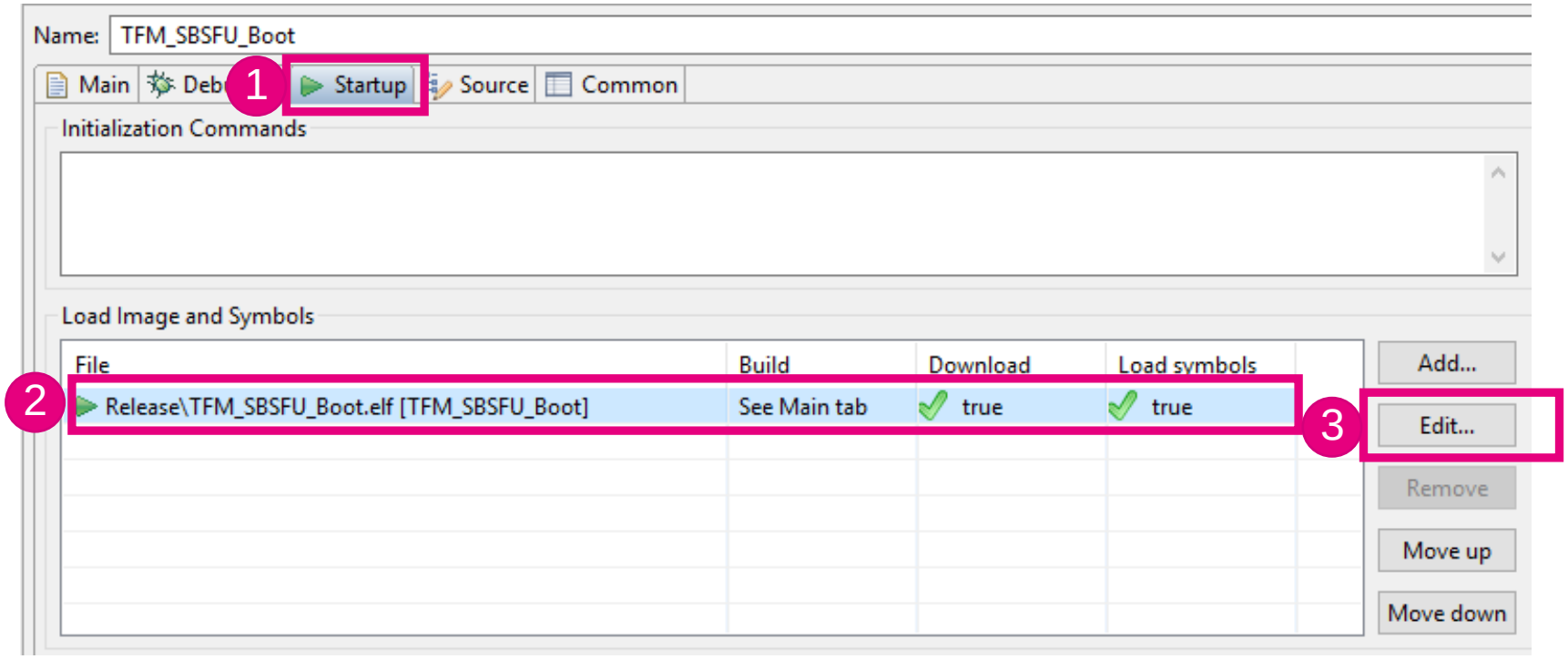
life.augmented

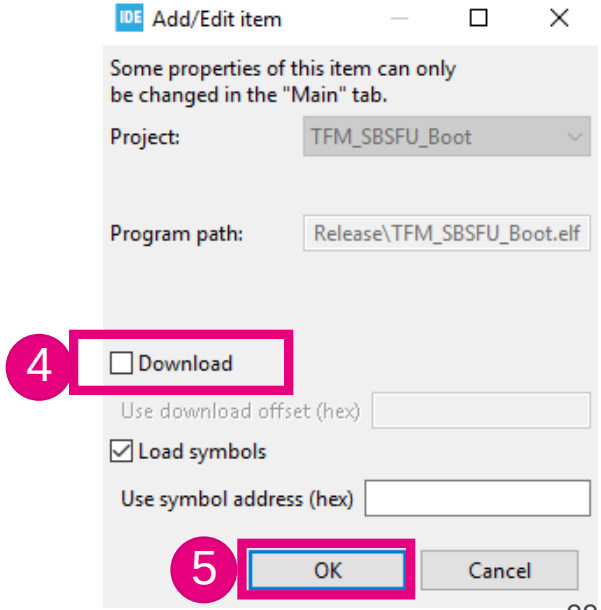
STM32CubeIDE debugging



STM32CubeIDE debugging

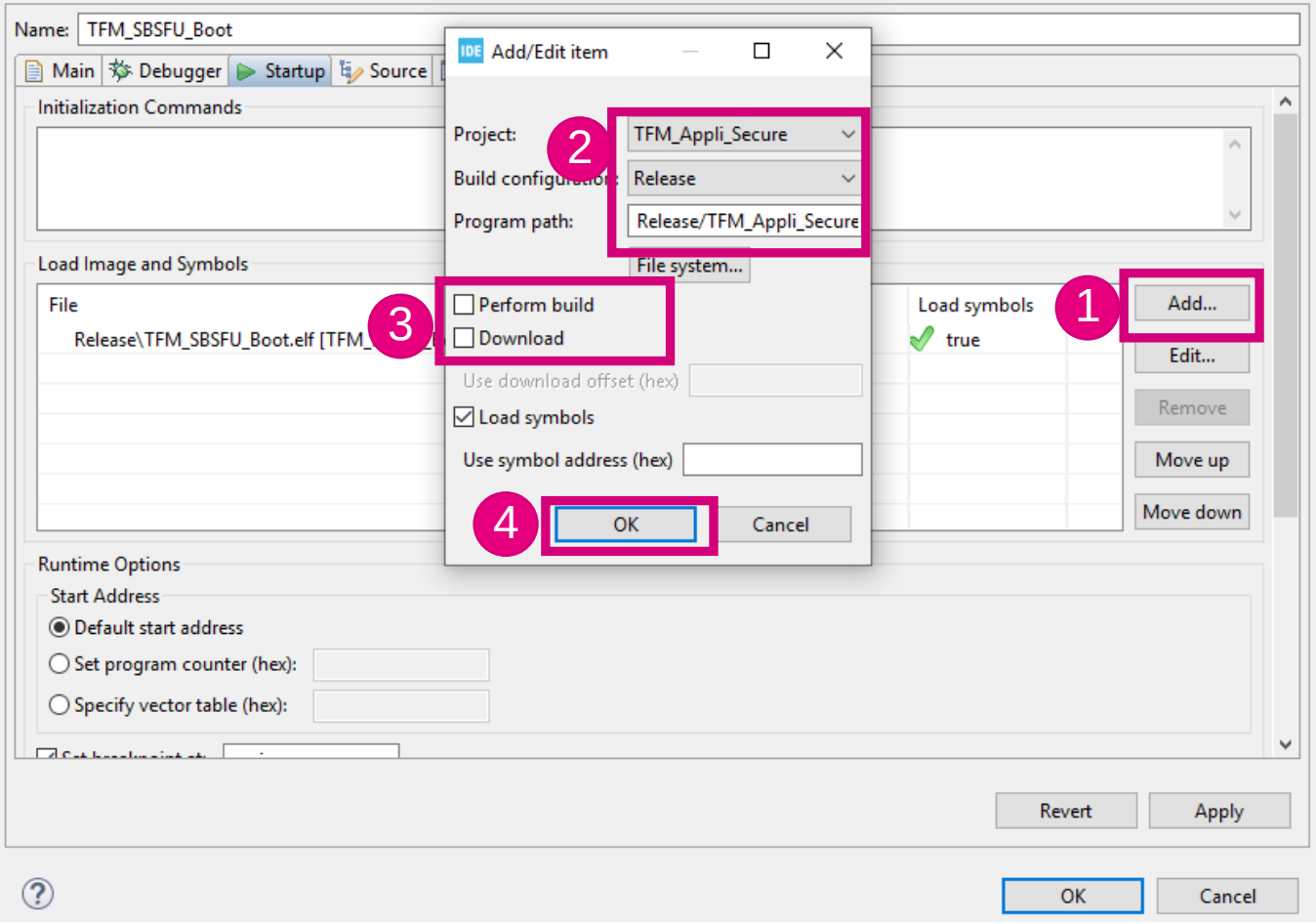
- Remove the SBSFU download





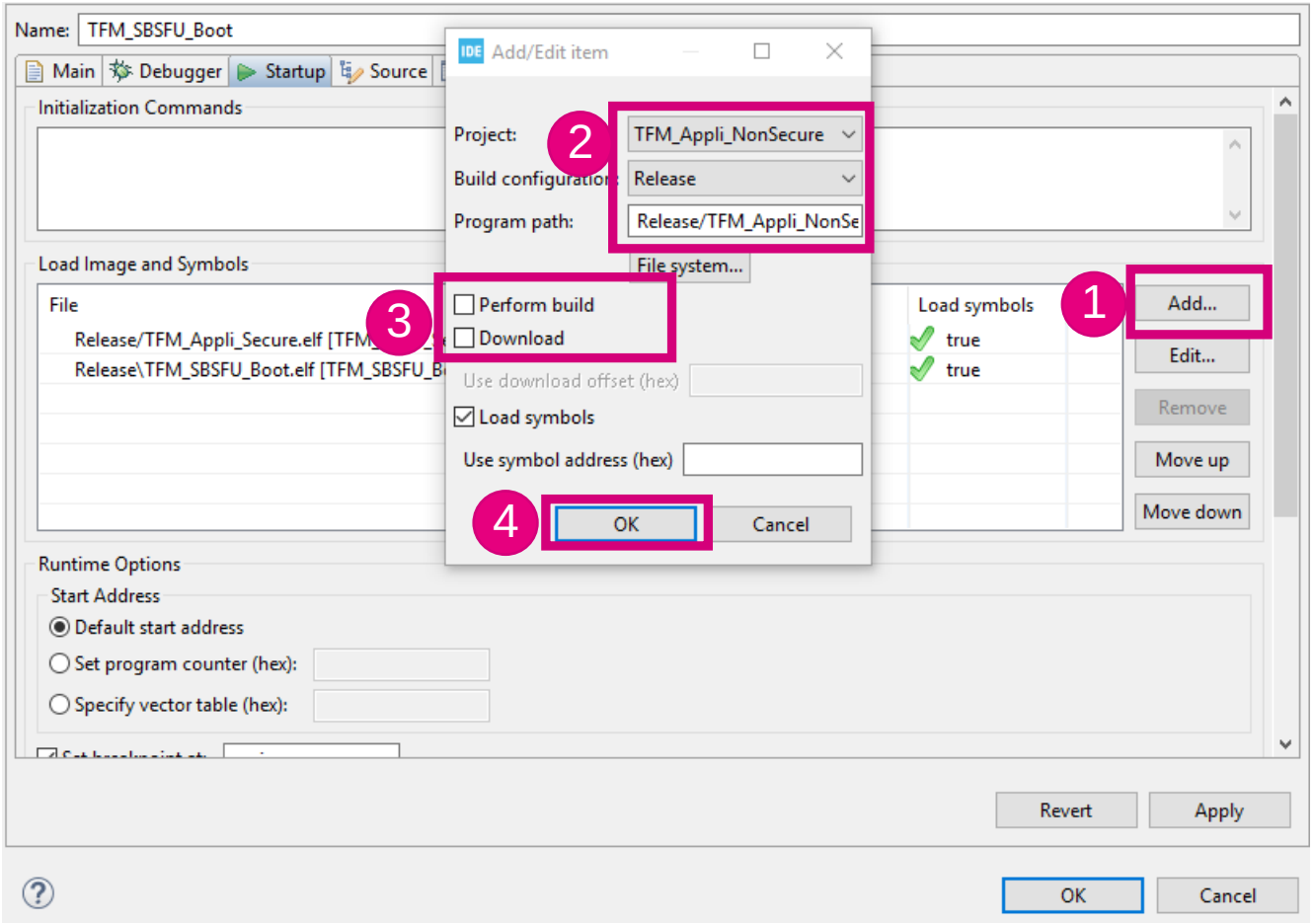
STM32CubeIDE debugging

- Add the Appli_Secure

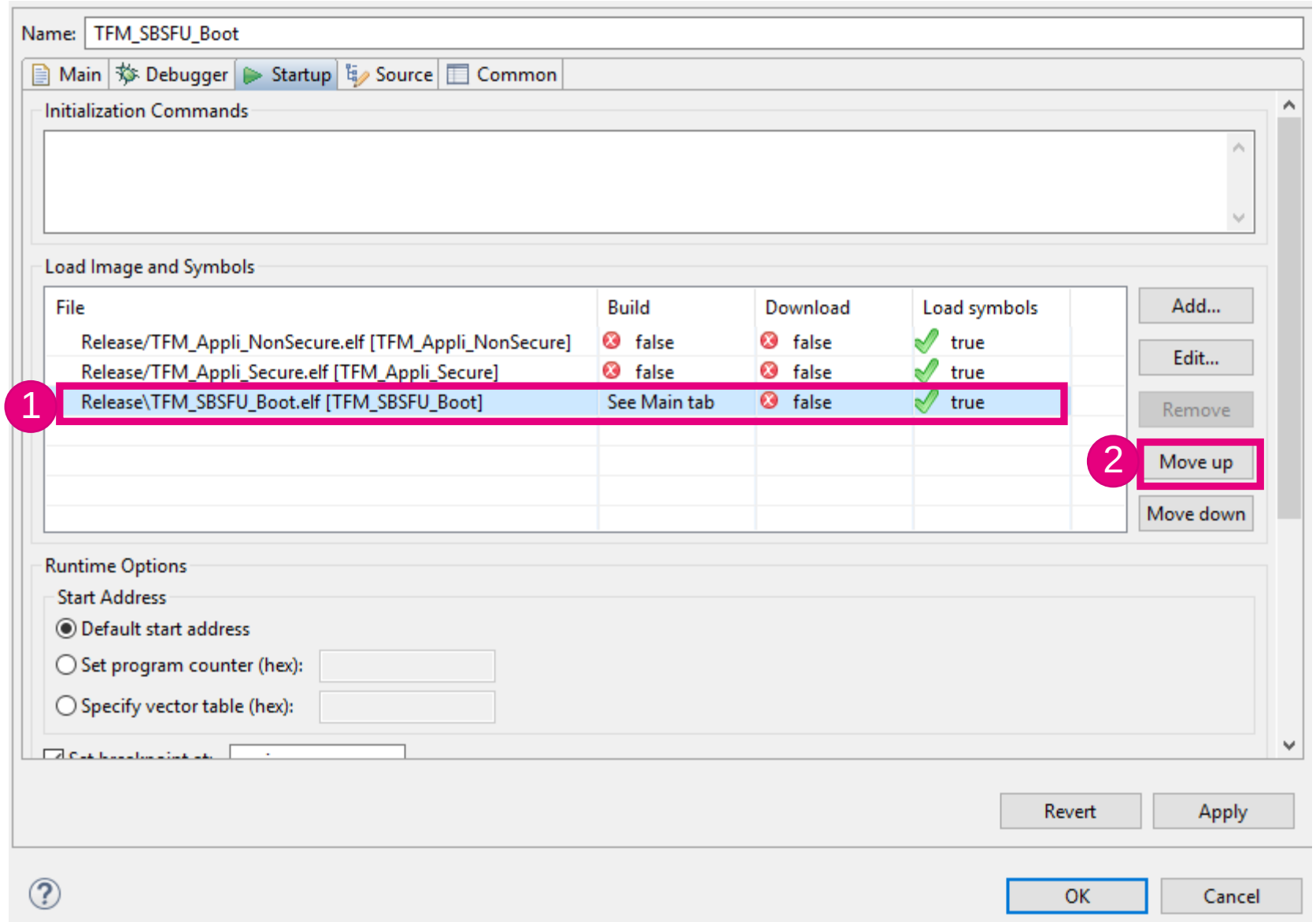


STM32CubeIDE debugging

- Add the Appli_NonSecure



STM32CubeIDE debugging



STM32CubeIDE debugging

Name: TFM_SBSFU_Boot

Main | Debugger | Startup | Source | Common

Initialization Commands

This order is important !

Load Image and Symbols

File	Build	Download	Load symbols
Release\TFM_SBSFU_Boot.elf [TFM_SBSFU_Boot]	See Main tab	false	true
Release/TFM_Appli_NonSecure.elf [TFM_Appli_NonSecure]	false	false	true
Release/TFM_Appli_Secure.elf [TFM_Appli_Secure]	false	false	true

Add... | Edit... | Remove | Move up | Move down

Runtime Options

Start Address

- (•) Default start address
- ( ) Set program counter (hex):
- ( ) Specify vector table (hex):

Revert | Apply

1 OK | Cancel

STM32CubeIDE debugging

STM32SecuWS - TFM_SBSFU_Boot/Middlewares/trustedfirmware/bl2_main.c - STM32CubeIDE

File Edit Source Refactor Navigate Search Project Run Window Help

Debug | Project Explorer

- TFM_SBSFU_Boot [STM32 Cortex-M C/C++ Application]
  - TFM_SBSFU_Boot.elf [cores: 0]
    - Thread #1 [main] 1 [core: 0] (Suspended : Breakpoint)
      - main() at bl2_main.c:180 0xc00a3d0
      - _start() at 0xc001b82
      - _start() at 0xc001b82
      - _start() at 0xc001b82
      - _start() at 0xc001b82
      - _start() at 0xc001b82
      - _start() at 0xc001b82
      - _start() at 0xc001b82
  - arm-none-eabi-gdb (8.1.0.20180315)
  - ST-LINK (ST-LINK GDB server)

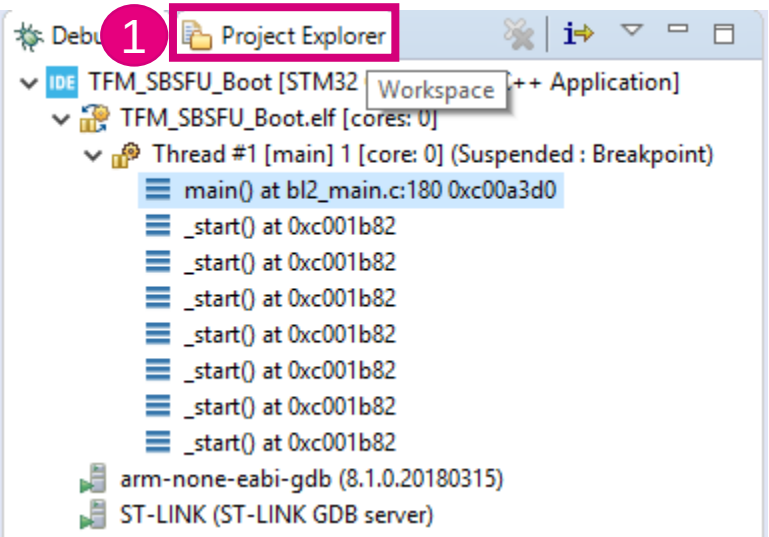
bl2_main.c | (gdb[1].proc[42000].threadGroup[i1],gdb[1].proc[42000].OSthread[1]).thread[1].frame[0]

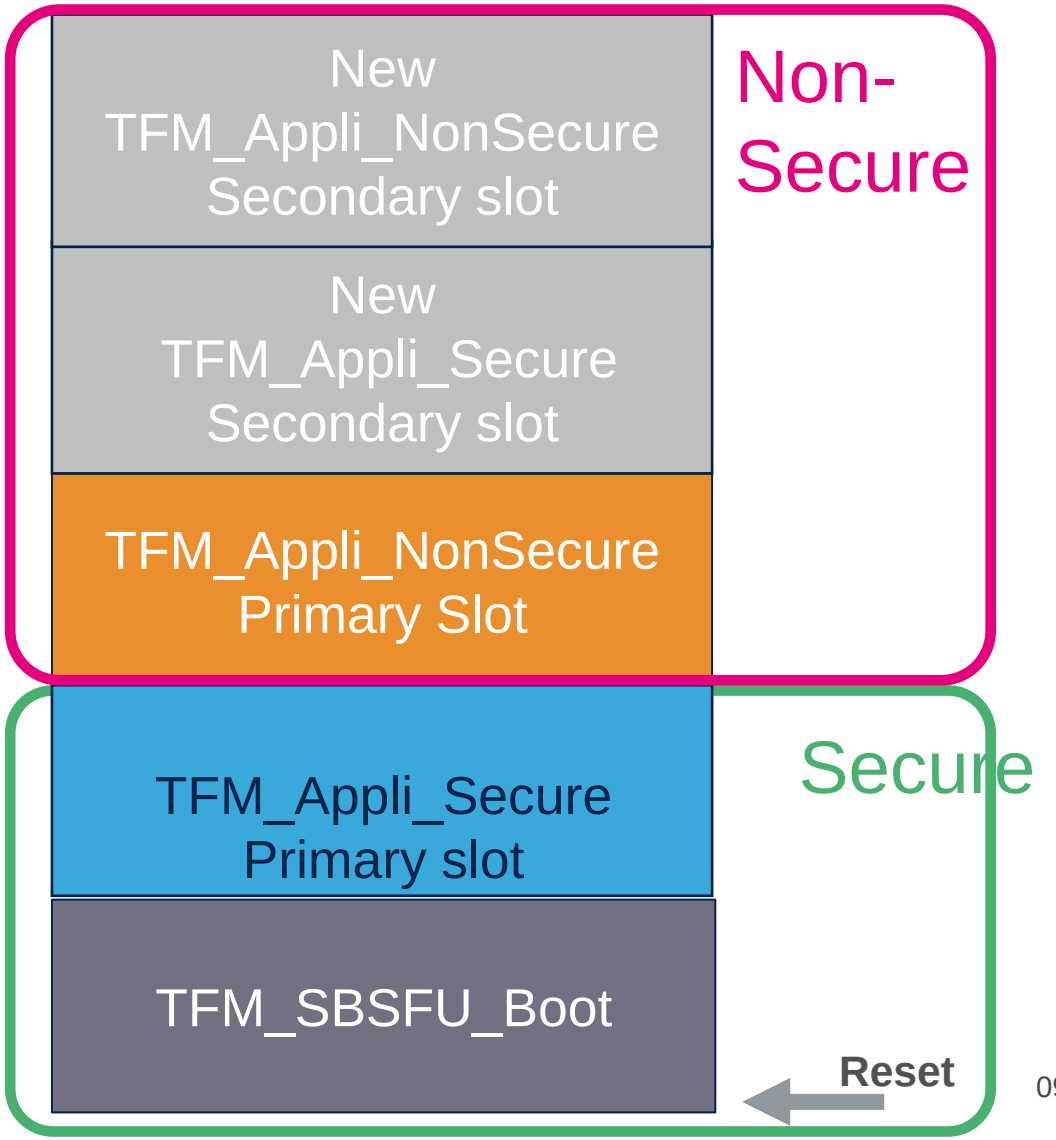
```
171      * bootloader transparent to it.
172      */
173     __set_MSPLIM(0);
174 #endif
175
176     jumper(vt);
177 }
178
179 int main(void)
180 {
181 #if defined(__ARM_ARCH_8M_MAIN__) || defined(__ARM_ARCH_8M_BASE__)
182     uint32_t msp_stack_bottom =
183             (uint32_t)&REGION_NAME(Image$$, ARM_LIB_STACK, $$ZI$$Base);
184 #endif
185     struct boot_rsp rsp;
186     int rc;
187
188 #if defined(__ARM_ARCH_8M_MAIN__) || defined(__ARM_ARCH_8M_BASE__)
189     __set_MSPLIM(msp_stack_bottom);
190 #endif
191
192     /* Perform platform specific initialization */
193     if (boot_platform_init() != 0) {
194         while (1)
195             ;
196     }
197
198 #if MCUBOOT_LOG_LEVEL > MCUBOOT_LOG_LEVEL_OFF
199     stdio_init();
200 #endif
201
202     BOOT_LOG_INF("Starting bootloader");
203
204     /* Initialise the mbedtls static memory allocator so that mbedtls allocates
```

life.augmented

STM32CubeIDE debugging

- Now we will put breakpoint in the main function of the TFM_Appli_Secure and just before the jump to the TFM_Appli_NonSecure.
- First switch to project explorer





Set breakpoint in the Appli_Secure

- TFM_Appli_Secure (in Secure)
  - Binaries
  - Includes
  - Application
  - Drivers
  - Middlewares
    - mbed-crypto
    - trustedfirmware
      - 1 core

2 tfm_core.c

```c
186 int main(void)
187 {
188     /* set Main Stack Pointer limit */
189     tfm_arch_set_msplim((uint32_t)&REGION_NAME(Image$$, ARM_LIB_STACK_MSP,
190                                                 $$ZI$$Base));
191
192     if (tfm_core_init() != TFM_SUCCESS) {
```

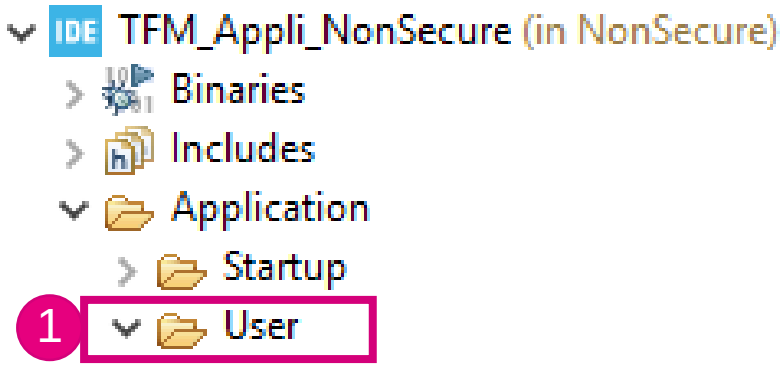
3

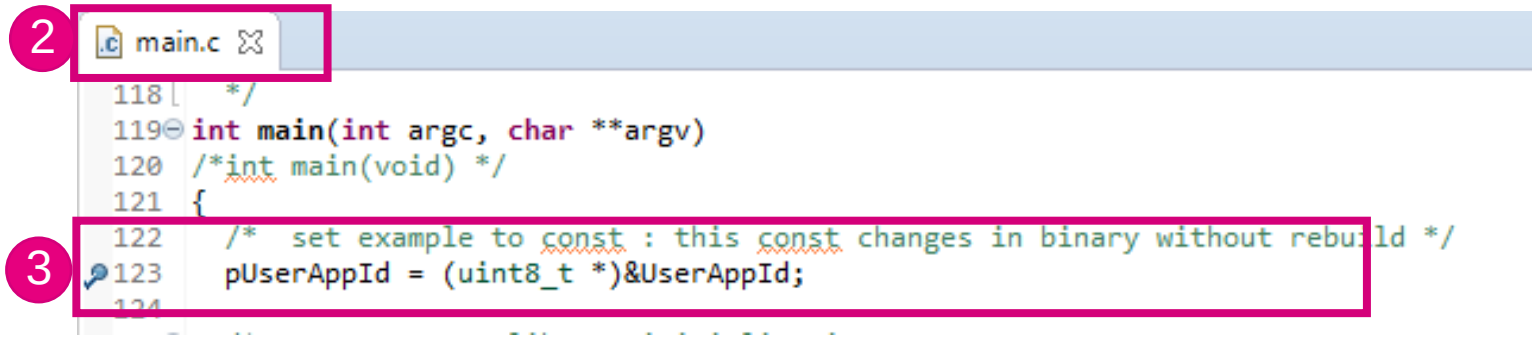
4 tfm_spm_services.c

```c
13 #include "secure_fw/include/tfm_spm_services_api.h"
14 #include "spm_api.h"
15 #include "psa/service.h"
16 #ifdef __ICCARM__
17 /* remove IAR warning relative to non void function not returning value */
18 #pragma diag_suppress=Pe940
19 #endif
20 nsfptr_t ns_entry;
21
22 void jump_to_ns_code(void)
23 {
24     /* calls the non-secure Reset_Handler to jump to the non-secure binary */
25     ns_entry();
26 }
```

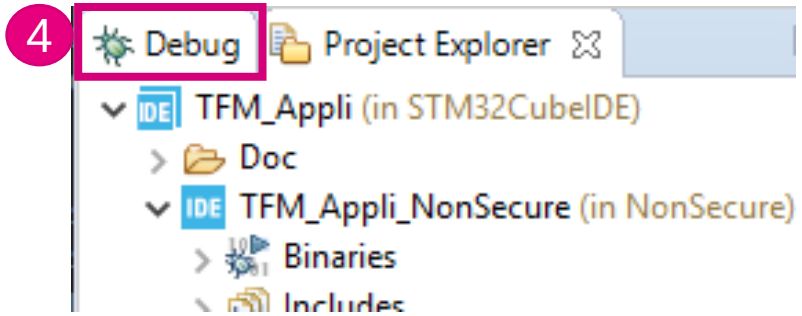
5

Set breakpoint in the Appli_NonSecure





- Switch to debug view



STM32CubeIDE debugging

File Edit Source Refactor Navigate Search Project Run Window Help

1

Debug | Project Expl...

- TFM_SBSFU_Boot [STM32 Cortex-M C/
  - TFM_SBSFU_Boot.elf [cores: 0]
    - Thread #1 [main] 1 [core: 0] (Susp
      - main() at bl2_main.c:180 0xc0
      - _start() at 0xc001b82
      - _start() at 0xc001b82
      - _start() at 0xc001b82
      - _start() at 0xc001b82
      - _start() at 0xc001b82
      - _start() at 0xc001b82
      - _start() at 0xc001b82
  - arm-none-eabi-gdb (8.1.0.20180315)
  - ST-LINK (ST-LINK GDB server)

bl2_main.c

```
178
179 int main(void)
180 {
181 #if defined(__ARM_ARCH_8M_MAIN__) || defined(__ARM_ARCH_8M_BASE__)
182     uint32_t msp_stack_bottom =
183             (uint32_t)&REGION_NAME(Image$$, ARM_LIB_STACK, $$ZI$$Base);
184 #endif
185     struct boot_rsp rsp;
186     int rc;
187
188 #if defined(__ARM_ARCH_8M_MAIN__) || defined(__ARM_ARCH_8M_BASE__)
189     __set_MSPLIM(msp_stack_bottom);
190 #endif
191
192     /* Perform platform specific initialization */
193     if (boot_platform_init() != 0) {
194         while (1)
195             ;
196     }
197
198 #if MCUBOOT_LOG_LEVEL > MCUBOOT_LOG_LEVEL_OFF
199     stdio_init();
```

Enter location here

```
                main:
0c00a3d0:         push    {r4, r5, lr}
 799              __ASM volatile ("MSR msp
0c00a3d2:         ldr     r3, [pc, #164]
180             {
0c00a3d4:         sub     sp, #20
0c00a3d6:         msr     MSPLIM, r3
193               if (boot_platform_init
0c00a3da:         bl      0xc0021ac <boot_
0c00a3de:         cbz     r0, 0xc00a3e2 <m
0c00a3e0:         b.n     0xc00a3e0 <main+
199               stdio_init();
0c00a3e2:         bl      0xc00a984 <stdic
202               BOOT_LOG_INF("Starting
0c00a3e6:         ldr     r0, [pc, #148]
0c00a3e8:         bl      0xc00acac <puts>
207               mbedtls_memory_buffer_
0c00a3ec:         mov.w   r1, #29184
```

Console | Problems | Executables | Debugger Console | Memory

TFM_SBSFU_Boot [STM32 Cortex-M C/C++ Application] ST-LINK (ST-LINK GDB server)

```
STMicroelectronics ST-LINK GDB server. Version 5.6.0
Copyright (c) 2020, STMicroelectronics. All rights reserved.

Starting server with the following options:
        Persistent Mode            : Disabled
        Logging Level              : 1
        Listen Port Number         : 61234
        Status Refresh Delay       : 15s
        Verbose Mode               : Disabled
        SWD Debug                  : Enabled
        InitWhile                  : Enabled
```

Read-Only | Smart Insert | 180 : 1 : 6328 | Secure

life.augmented

STM32CubeIDE debugging

STM32SecuWS - TFM_Appli_Secure/Middlewares/trustedfirmware/core/tfm_core.c - STM32CubeIDE

File Edit Source Refactor Navigate Search Project Run Window Help

1

Debug | Project Expl...

- TFM_SBSFU_Boot [STM32 Cortex-M C/
  - TFM_SBSFU_Boot.elf [cores: 0]
    - Thread #1 [main] 1 [core: 0] (Susp
      - main() at tfm_core.c:192 0xc03
  - arm-none-eabi-gdb (8.1.0.20180315)
  - ST-LINK (ST-LINK GDB server)

bl2_main.c | tfm_core.c

```c
    default:
        *res_ptr = (uint32_t)TFM_ERROR_INVALID_PARAMETER;
    }
}
#endif /* TFM_PSA_API */

int main(void)
{
    /* set Main Stack Pointer limit */
    tfm_arch_set_msplim((uint32_t)&REGION_NAME(Image$$, ARM_LIB_STACK_MSP,
                                                $$ZI$$Base));

    if (tfm_core_init() != TFM_SUCCESS) {
        tfm_panic();
    }

    if (tfm_spm_db_init() != SPM_ERR_OK) {
        tfm_panic();
    }

#if TFM_LVL != 1
    if (tfm_spm_hal_setup_isolation_hw() != TFM_PLAT_ERR_SUCCESS) {
```

Enter location here

```
0c031608:   bl      0xc031554 <tfm_core_init>
0c03160c:   cbz     r0, 0xc031612 <main+18>
193               tfm_panic();
0c03160e:   bl      0xc032a70 <tfm_panic>
196           if (tfm_spm_db_init() != SPM_ER
0c031612:   bl      0xc02f5c4 <tfm_spm_db_ini
0c031616:   cbz     r0, 0xc03161c <main+28>
197               tfm_panic();
0c031618:   bl      0xc032a70 <tfm_panic>
201           if (tfm_spm_hal_setup_isolatior
0c03161c:   bl      0xc019e70 <tfm_spm_hal_se
0c031620:   cbz     r0, 0xc031626 <main+38>
202               tfm_panic();
0c031622:   bl      0xc032a70 <tfm_panic>
139           tfm_arch_prioritize_secure_exce
0c031626:   bl      0xc03123c <tfm_arch_prior
142           plat_err = tfm_spm_hal_set_secu
0c03162a:   movs    r1, #0
```

You will stop in the main of TFM_Appli_Secure

STM32CubeIDE debugging

STM32SecuWS - TFM_Appli_Secure/Middlewares/trustedfirmware/core/tfm_spm_services.c - STM32CubeIDE

File Edit Source Refactor Navigate Search Project Run Window Help

1

Debug | Project Expl...

- TFM_SBSFU_Boot [STM32 Cortex-M C/
  - TFM_SBSFU_Boot.elf [cores: 0]
    - Thread #1 [main] 1 [core: 0] (Susp
      - jump_to_ns_code() at tfm_spn
      - tfm_nspm_thread_entry() at tf
      - tfm_psa_close_veneer() at tfm_
      - 0x0
  - arm-none-eabi-gdb (8.1.0.20180315)
  - ST-LINK (ST-LINK GDB server)

bl2_main.c | tfm_core.c | main.c | tfm_spm_services.c

```c
19  #endif
20  nsfptr_t ns_entry;
21
22  void jump_to_ns_code(void)
23  {
24      /* Calls the non-secure Reset_Handler to jump to the non-secure binary */
25      ns_entry();
26  }
27
28  #ifndef TFM_PSA_API
29  __attribute__((naked))
30  int32_t tfm_core_memory_permission_check(const void *ptr,
31                                           uint32_t len,
32                                           int32_t access)
33  {
34    __ASM volatile(
35          "SVC    %0\n"
36          "BX     lr\n"
37          : : "I" (TFM_SVC_MEMORY_CHECK));
38  }
39
40  __attribute__((naked))
```

You will stop just before the call to the TFM_Appli_NonSecure

life.augmented

STM32CubeIDE debugging

STM32SecuWS - Source not found. - STM32CubeIDE

File Edit Navigate Search Project Run Window Help

1

Debug | Project Explorer

- TFM_SBSFU_Boot [STM32 Cortex-M C/C
  - TFM_SBSFU_Boot.elf [cores: 0]
    - Thread #1 [main] 1 [core: 0] (Suspe
      - __gnu_cmse_nonsecure_call() at
      - jump_to_ns_code() at tfm_spm_
      - tfm_nspm_thread_entry() at tfm
      - tfm_psa_close_veneer() at tfm_p
      - 0x0
  - arm-none-eabi-gdb (8.1.0.20180315)
  - ST-LINK (ST-LINK GDB server)

tfm_spm_serv... | __gnu_cmse_n...

No source available for "__gnu_cmse_nonsecure_call() at 0xc018902"

View Disassembly...

Configure when this editor is shown Preferences...

(x)= Varia... | Break... | Expre... | Modu... | Disas... | Regis...

Enter location here

```
__gnu_cmse_nonsecure_call:
0c0188e4:  stmdb   sp!, {r5, r6, r7, r8, r9, r10, r11, lr}
0c0188e8:  mov     r7, r4
0c0188ea:  mov     r8, r4
0c0188ec:  mov     r9, r4
0c0188ee:  mov     r10, r4
0c0188f0:  mov     r11, r4
0c0188f2:  mov     r12, r4
0c0188f4:  sub     sp, #136        ; 0x88
0c0188f6:  vlstm   sp
0c0188fa:  msr     CPSR_f, r4
0c0188fe:  mov     r5, r4
0c018900:  mov     r6, r4
0c018902:  blxns   r4
0c018904:  vlldm   sp
0c018908:  add     sp, #136        ; 0x88
0c01890a:  ldmia.w sp!, {r5, r6, r7, r8, r9, r10, r11, pc}
0c01890e:  movs    r0, r0
__aeabi_drsub:
0c018910:  eor.w   r1, r1, #2147483648     ; 0x80000000
```

Use the « Step in » to find the blxns intruction.
Then do an additional « Step in » and observe the processor state.

life.augmented

STM32CubeIDE debugging

STM32SecuWS - TFM_Appli_NonSecure/Application/Startup/startup_stm32l5xx_ns.S - STM32CubeIDE

File Edit Navigate Search Project Run Window Help

2

Debug | Project Explorer

- TFM_SBSFU_Boot [STM32 Cortex-M C/C
  - TFM_SBSFU_Boot.elf [cores: 0]
    - Thread #1 [main] 1 [core: 0] (Suspe
      - Reset_Handler() at startup_stm3
      - 0xfeffffe
  - arm-none-eabi-gdb (8.1.0.20180315)
  - ST-LINK (ST-LINK GDB server)

__gnu_cmse_n... | startup_stm...

```
179     ldr     r4, =__copy_table_start__
180     ldr     r5, =__copy_table_end__
181
182 .L_loop0:
183     cmp     r4, r5
184     bge     .L_loop0_done
185     ldr     r1, [r4]
186     ldr     r2, [r4, #4]
187     ldr     r3, [r4, #8]
188
189 .L_loop0_0:
190     subs    r3, #4
191     ittt    ge
192     ldrge   r0, [r1, r3]
193     strge   r0, [r2, r3]
194     bge     .L_loop0_0
195
196     adds    r4, #12
197     b       .L_loop0
198
199 .L_loop0_done:
200
```

Quick Access | (x)= Varia... | Break... | Expre... | Modu... | Disas... | Regis... | Live ...

Enter location here

```
Reset_Handler:
080386a8:   ldr     r4, [pc, #60]   ; (0x80386e8 <Reset_Handler+64>)
180           ldr     r5, =__copy_table_end__
080386aa:   ldr     r5, [pc, #64]   ; (0x80386ec <Reset_Handler+68>)
183           cmp     r4, r5
080386ac:   cmp     r4, r5
184           bge     .L_loop0_done
080386ae:   bge.n   0x80386c4 <Reset_Handler+28>
185           ldr     r1, [r4]
080386b0:   ldr     r1, [r4, #0]
186           ldr     r2, [r4, #4]
080386b2:   ldr     r2, [r4, #4]
187           ldr     r3, [r4, #8]
080386b4:   ldr     r3, [r4, #8]
190           subs    r3, #4
080386b6:   subs    r3, #4
191           ittt    ge
080386b8:   ittt    ge
192           ldrge   r0, [r1, r3]
080386ba:   ldrge   r0, [r1, r3]
```

Console | Problems | Executables | Debugger Console | Memory

TFM_SBSFU_Boot [STM32 Cortex-M C/C++ Application] ST-LINK (ST-LINK GDB server)

```
STMicroelectronics ST-LINK GDB server. Version 5.6.0
Copyright (c) 2020, STMicroelectronics. All rights reserved.

Starting server with the following options:
        Persistent Mode            : Disabled
        Logging Level              : 1
        Listen Port Number         : 61234
        Status Refresh Delay       : 15s
        Verbose Mode               : Disabled
        SWD Debug                  : Enabled
        InitWhile                  : Enabled
```

1 Non-Secure

life.augmented

STM32CubeIDE debugging

STM32SecuWS - TFM_Appli_NonSecure/Application/User/main.c - STM32CubeIDE

File Edit Source Refactor Navigate Search Project Run Window Help

Debug | Project Explorer

- TFM_SBSFU_Boot [STM32 Cortex-M C/C
  - TFM_SBSFU_Boot.elf [cores: 0]
    - Thread #1 [main] 1 [core: 0] (Suspe
      - main() at main.c:123 0x8038ffa
      - _start() at 0x8038682
  - arm-none-eabi-gdb (8.1.0.20180315)
  - ST-LINK (ST-LINK GDB server)

bl2_main.c | tfm_core.c | main.c | tfm_spm_servic... | __gnu_cmse_non... | startup_stm32l...

```c
114 /**
115   * @brief  Main program
116   * @param  None
117   * @retval None
118   */
119 int main(int argc, char **argv)
120 /*int main(void) */
121 {
122   /*  set example to const : this const changes in binary without rebuild */
123   pUserAppId = (uint8_t *)&UserAppId;
124
125   /* STM32L5xx HAL library initialization:
126   - Systick timer is configured by default as source of time base, but user
127   can eventually implement his proper time base source (a general purpose
128   timer for example or other time source), keeping in mind that Time base
129   duration should be kept 1ms since PPP_TIMEOUT_VALUEs are defined and
130   handled in milliseconds basis.
131   - Set NVIC Group Priority to 3
132   - Low Level Initialization
133   */
134   HAL_Init();
135
```

STM32CubeIDE debugging

- Terminate debugging session  or CTRL+F2

life.augmented

Where do we stand ?

- So we experimented TFM-SBSFU functionalities.
- We compile and debug TFM_SBSFU_Boot / TFM Appli Secure / TFM Appli NonSecure
- Next possible hands-On
  - Activate HDP
  - Activate RDP 0.5
- If you stop here, please go to slide “Board clean up!” (at the end of this presentation)

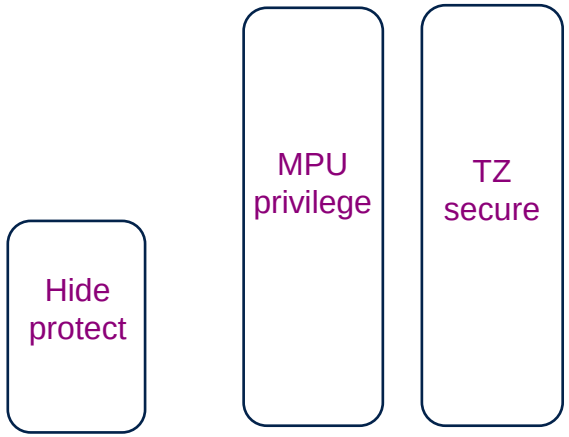
life.augmented

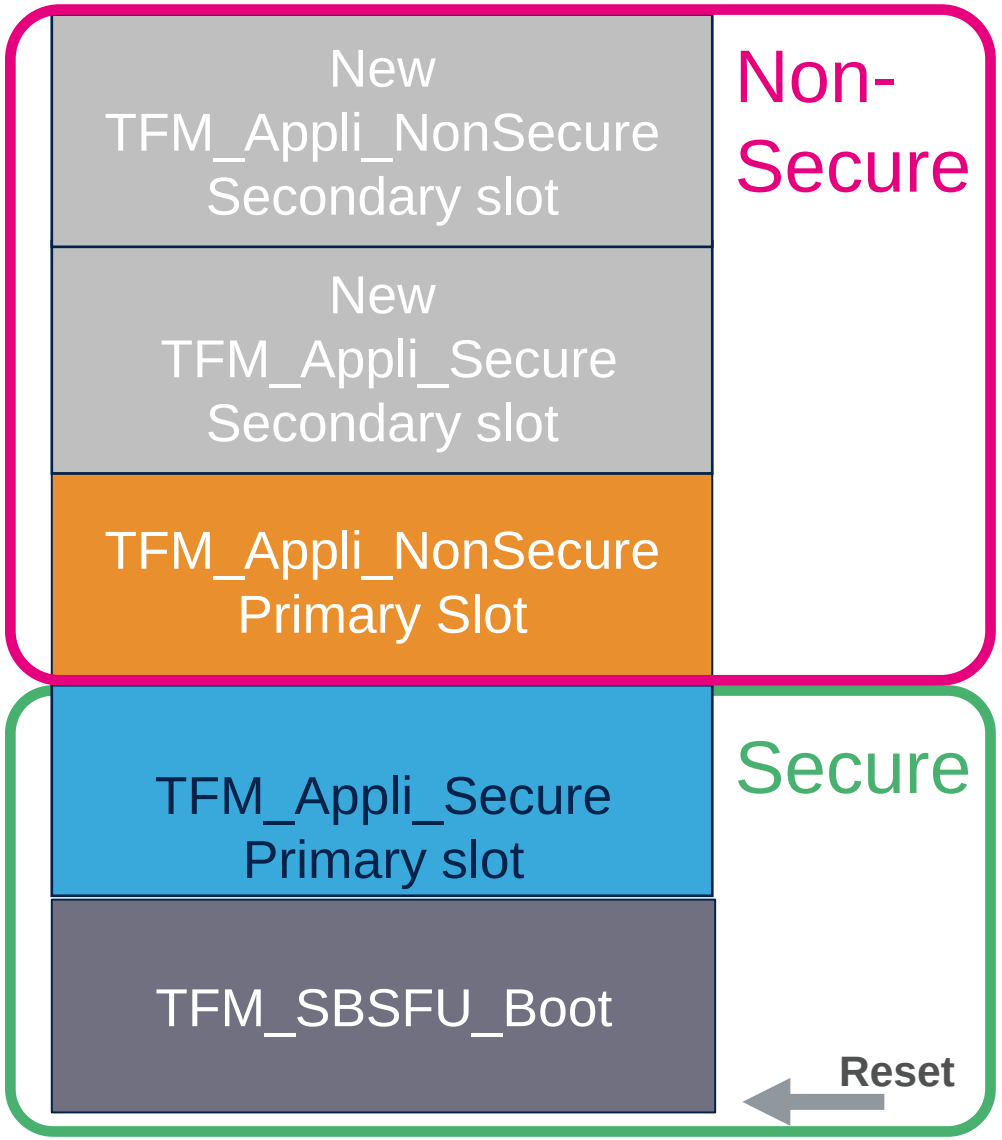
HDP activation

Let’s activate the HDP !

Purpose : Add an new level of isolation for the TFM_SBSFU.

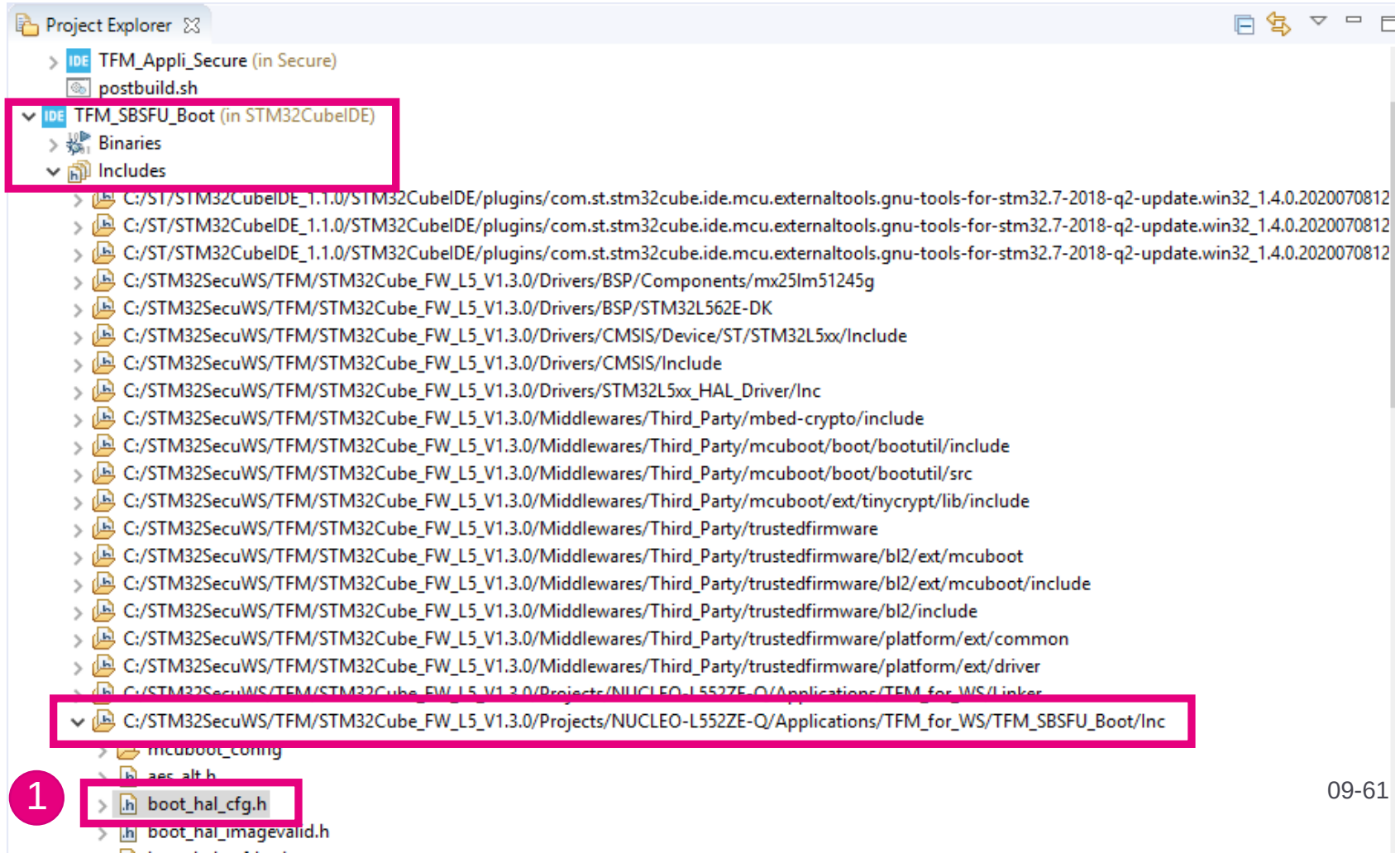
Scenario :
1- activate and configure the HDP (code flag + option byte)
2- check access to TFM_SBSFU code





HDP activation

- In the TFM_SBSFU_Boot, please open file boot_hal_cfg.h



life.augmented

HDPactivation

- In the opened file boot_hal_cfg.h
- Uncomment line 41:

*boot_hal_cfg.h

```
25
26 /* Includes ------------------------------------------------------------------
27 #include "stm32l5xx_hal.h"
28 #define RTC_CLOCK_SOURCE_LSE
29
30
31 #ifdef RTC_CLOCK_SOURCE_LSE
32 #define RTC_ASYNCH_PREDIV  0x7F
33 #define RTC_SYNCH_PREDIV   0x00FF
34 #endif /* RTC_CLOCK_SOURCE_LSE */
35
36 /* ICache */
37 #define TFM_ICACHE_ENABLE /*!< Instruction cache enable */
38
39 /* Static protection checking  Flag */
40 //#define TFM_WRP_PROTECT_ENABLE  /*!< Write Protection  */
41 #define TFM_HDP_PROTECT_ENABLE /*!< HDP protection   */
42 //#define  TFM_OB_RDP_LEVEL_VALUE OB_RDP_LEVEL_1 /*!< RDP level */
43 #define TFM_SECURE_USER_SRAM2_ERASE_AT_RESET /*!< SRAM2 clear at Reset  */
44 #ifdef TFM_DEV_MODE
45 #define TFM_OB_BOOT_LOCK 0 /*!< BOOT Lock expected value  */
```

- Save the file and compile the TFM_SBSFU_Boot 
- Flash the TFM_SBSFU_Boot

C:\STM32SecuWS\TFM\Scripts

STEP6_flash_SBSFU_binary.bat

life.augmented

Testing HDP (Secure hide protection)

- We must set the option byte associated :

  HDP1EN to 1

  HDP1_PEND to 0x1C -> 0x0800E000

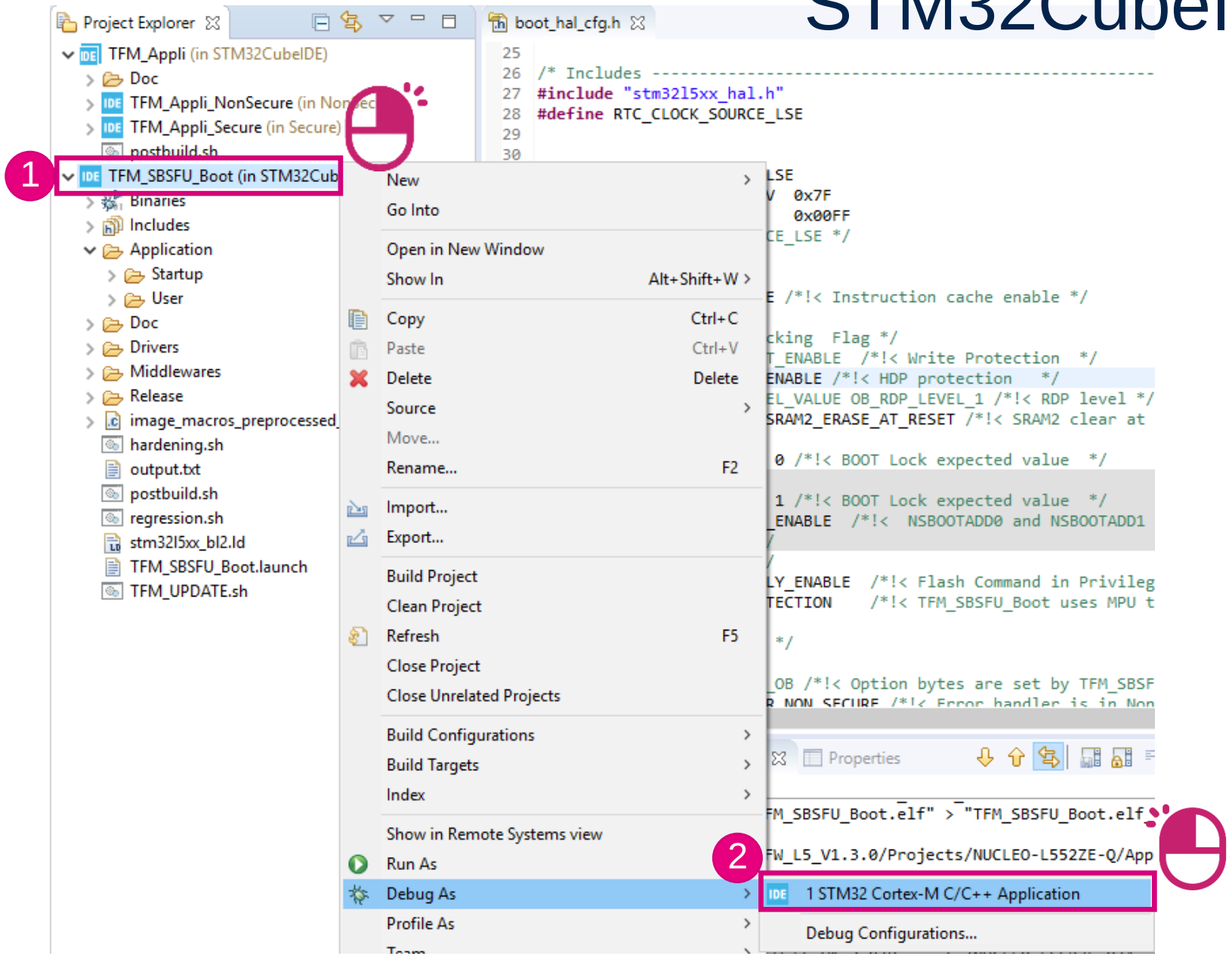
C:\STM32SecuWS\TFM\Scripts

- STEP7_configure_HDP.bat

C:\windows\system32\cmd.exe

```
Reconnecting...
Reconnected !


UPLOADING OPTION BYTES DATA ...

  Bank           : 0x00
  Address        : 0x50022040
  Size           : 32 Bytes

                                                    100%

  Bank           : 0x01
  Address        : 0x50022060
  Size           : 16 Bytes

                                                    100%

OPTION BYTE PROGRAMMING VERIFICATION:

Option Bytes successfully programmed

"*****************************************************************"
"Option setting"
"*****************************************************************"
"HDP1EN             : enabled "
"HDP1_PEND          : 0x1C  -> 0x0800E000 "
"*****************************************************************"
"Board is ready to receive the TFM binaries, press key"
Press any key to continue . . .
```

STM32CubeIDE debugging



life.augmented

STM32CubeIDE debugging

STM32SecuWS - TFM_SBSFU_Boot/Middlewares/trustedfirmware/bl2_main.c - STM32CubeIDE

File Edit Source Refactor Navigate Search Project Run Window Help

Debug | Project Explorer

- TFM_SBSFU_Boot [STM32 Cortex-M C/C++ Appl
  - TFM_SBSFU_Boot.elf [cores: 0]
    - Thread #1 [main] 1 [core: 0] (Suspended : E
      - main() at bl2_main.c:180 0xc00a3f4
      - _start() at 0xc001b82
      - _start() at 0xc001b82
      - _start() at 0xc001b82
      - _start() at 0xc001b82
      - _start() at 0xc001b82
      - _start() at 0xc001b82
      - _start() at 0xc001b82
  - arm-none-eabi-gdb (8.1.0.20180315)
  - ST-LINK (ST-LINK GDB server)

boot_hal_cfg.h | (gdb[2].proc[42000].threadGroup[i1],gdb[2].proc[42000].OSthread[1]).thread[1].frame[0] | bl2_main.c

```
173     __set_MSPLIM(0);
174 #endif
175
176     jumper(vt);
177 }
178
179 int main(void)
180 {
181 #if defined(__ARM_ARCH_8M_MAIN__) || defined(__ARM_ARCH_8M_BASE__)
182     uint32_t msp_stack_bottom =
183             (uint32_t)&REGION_NAME(Image$$, ARM_LIB_STACK, $$ZI$$Base);
184 #endif
185     struct boot_rsp rsp;
186     int rc;
187
188 #if defined(__ARM_ARCH_8M_MAIN__) || defined(__ARM_ARCH_8M_BASE__)
189     __set_MSPLIM(msp_stack_bottom);
190 #endif
191
```

Console | Problems | Executables | Debugger Cons | Memory

1

Monitors

2

0x0C001000

0x0C001000 : 0x0C001000 <Hex> | New Renderings...

Address	0 - 3	4 - 7	8 - B	C - F
0C001000	5F53544D	33324C36	35325858	5F48554B
0C001010	5F435553	544F4D49	5A415449	4F4E5F0D
0C001020	0079EBA9	0E8BF450	A6751576	AD4599B0
0C001030	7ADF938D	A3BB0BD1	7D0036ED	49A2D0FC

life.augmented

STM32CubeIDE debugging

- Run  (it should stop on the Appli Secure previously set)

STM32SecuWS - TFM_Appli_Secure/Middlewares/trustedfirmware/core/tfm_core.c - STM32CubeIDE

File Edit Source Refactor Navigate Search Project Run Window Help

Debug | Project Explorer

- TFM_SBSFU_Boot [STM32 Cortex-M C/C++ Appl
  - TFM_SBSFU_Boot.elf [cores: 0]
    - Thread #1 [main] 1 [core: 0] (Suspended : E
      - main() at tfm_core.c:192 0xc031608
  - arm-none-eabi-gdb (8.1.0.20180315)
  - ST-LINK (ST-LINK GDB server)

boot_hal_cfg.h | (gdb[2].proc[42000].threadGroup[i1],gdb[2].proc[42000].OSthread[1]).thread[1].frame[0] | bl2_main.c

```
185
186 int main(void)
187 {
188     /* set Main Stack Pointer limit */
189     tfm_arch_set_msplim((uint32_t)&REGION_NAME(Image$$, ARM_LIB_STACK_MSP,
190                                                 $$ZI$$Base));
191
192     if (tfm_core_init() != TFM_SUCCESS) {
193         tfm_panic();
194     }
195
196     if (tfm_spm_db_init() != SPM_ERR_OK) {
197         tfm_panic();
198     }
199
200 #if TFM_LVL != 1
201     if (tfm_spm_hal_setup_isolation_hw() != TFM_PLAT_ERR_SUCCESS) {
202         tfm_panic();
203     }
204 #endif /* TFM_LVL != 1 */
```

Console | Problems | Executables | Debugger Console | Memory

Monitors: 0x0C001000

0x0C001000 : 0x0C001000 <Hex> | New Renderings...

Address	0 - 3	4 - 7	8 - B	C - F
0C001000	00000000	00000000	00000000	00000000
0C001010	00000000	00000000	00000000	00000000
0C001020	00000000	00000000	00000000	00000000
0C001030	00000000	00000000	00000000	00000000
0C001040	00000000	00000000	00000000	00000000

0x0C001000

life.augmented

STM32CubeIDE debugging

- Terminate debugging session  or CTRL+F2

life.augmented

Where do we stand?

- So we experimented TFM-SBSFU functionalities.
- We compile and debug TFM_SBSFU_Boot / TFM Appli Secure / TFM Appli Non-secure
- We activate HDP and we experiment this functionality
- Next possible hands-On
  - Activate RDP 0.5
- If you stop here, please go to slide “Board clean up!” (at the end of this presentation)

life.augmented

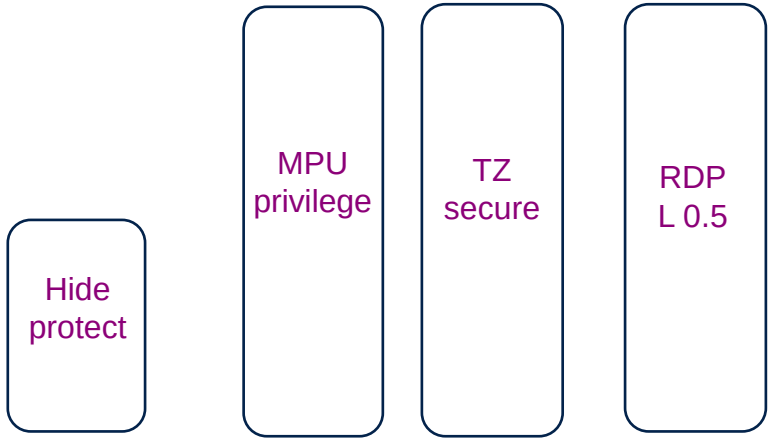
RDP 0.5 activation

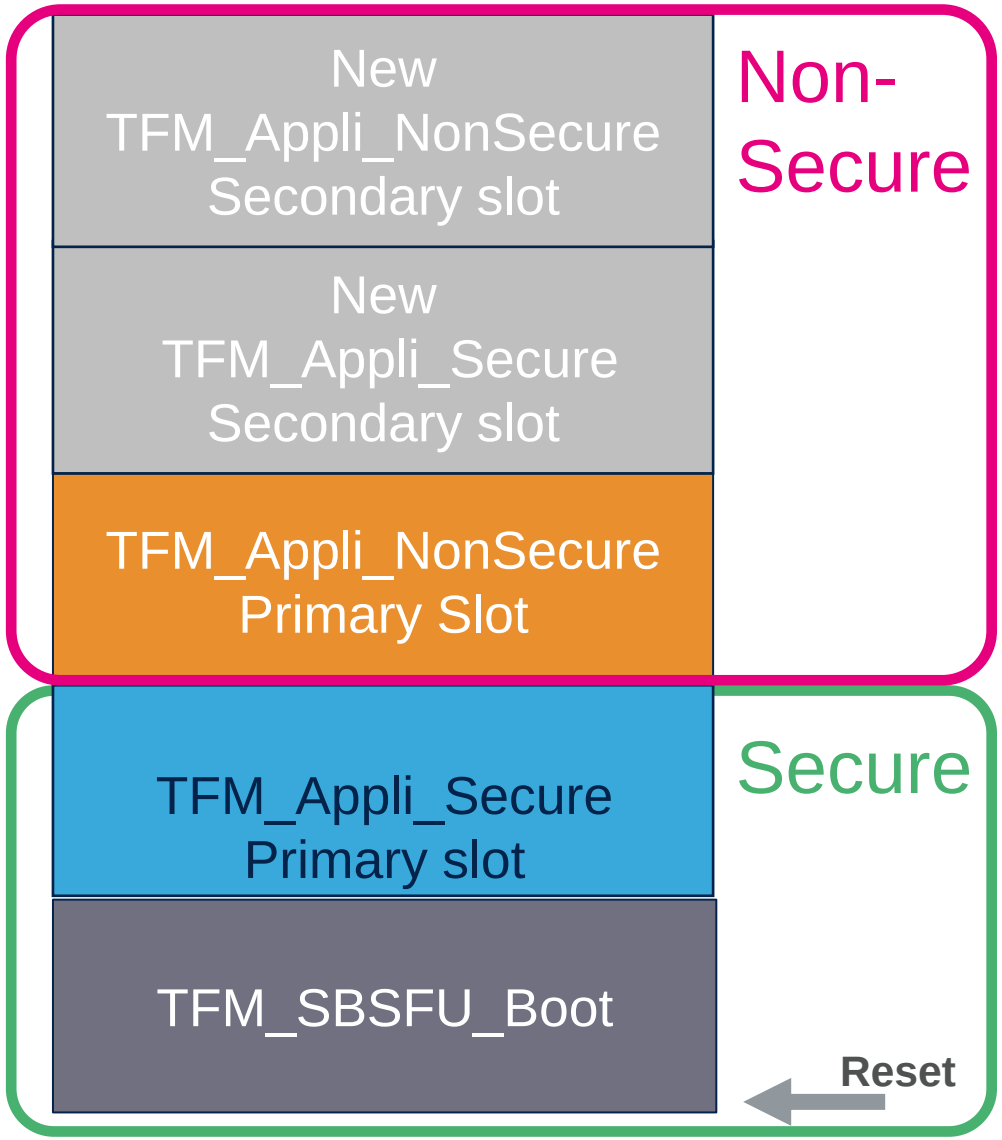
life.augmented

Let’s activate the RDP 0.5 !

Purpose : allow debuging only the non secure part.

Question : what should I insure before going to RDP 0.5 ?





RDP 0.5 warning !

- RDP 0.5 : non-secure debug only
  - The debug access to secure area is prohibited, so you must insure the secure code properly jump in the non-secure application
- Check with Teraterm

COM20 - Tera Term VT

File Edit Setup Control Window Help

```
[INF] Starting bootloader
[INF] Checking BL2 NV area
[INF] Checking BL2 NV area header
[INF] Checking BL2 NV Counter consitency
[INF] Consistent BL2 NV Counter 3  = 0x1000000
[INF] Consistent BL2 NV Counter 4  = 0x1000000
[INF] Swap type: none
[INF] Swap type: none
[INF] verify counter  0 1000000 1000000
[INF] counter  0 : ok
[INF] verify sig key id 0
[INF] signature OK
[INF] verify counter  1 1000000 1000000
[INF] counter  1 : ok
[INF] verify sig key id 1
[INF] signature OK
[INF] Bootloader chainload address offset: 0x14000
[INF] Jumping to the first image slot
[INF] BL2 HUK _STM32L652XX_HUK_CUSTOMIZATION_
 set to BL2 SHARED DATA
[INF] Code c001900 c00ea9e
[INF] hash TFM_SBSFU_Boot  d1ed135 .. 685366e8
[Sec Thread] Secure image initializing!

=================================================================
=              (C) COPYRIGHT 2019 STMicroelectronics            =
=                                                               =
=                         User App #A                           =
=================================================================


=================== Main Menu ============================

  Test Protections ------------------------------------- 1

  Test TFM --------------------------------------------- 2

  Download a new Fw Image ------------------------------ 3

  Selection :
```

RDP 0.5 activation

- We must set the option byte associated :

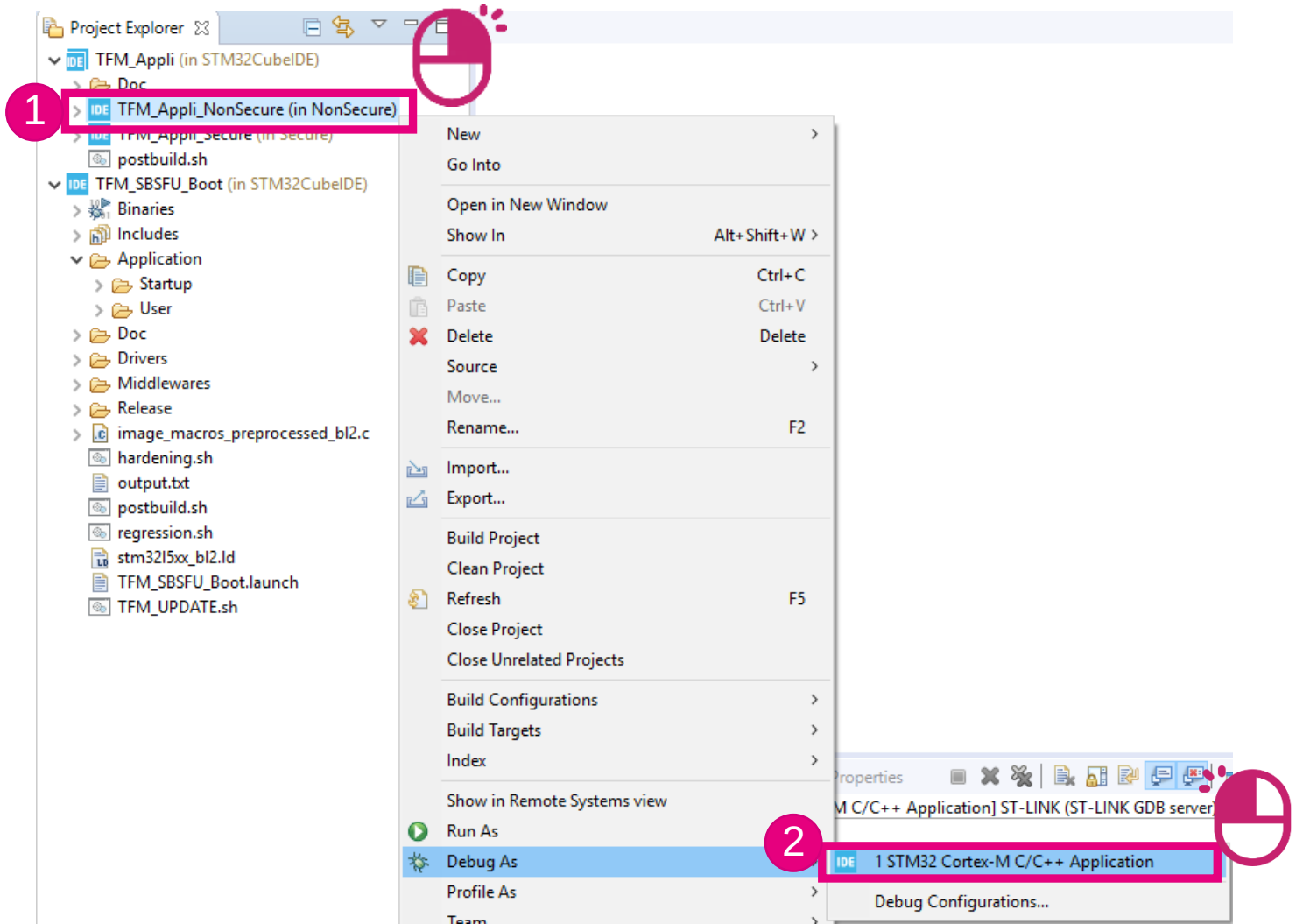
  RDP to 0x55

C:\STM32SecuWS\TFM\Scripts

- STEP8_activate_RDP_0_5.bat

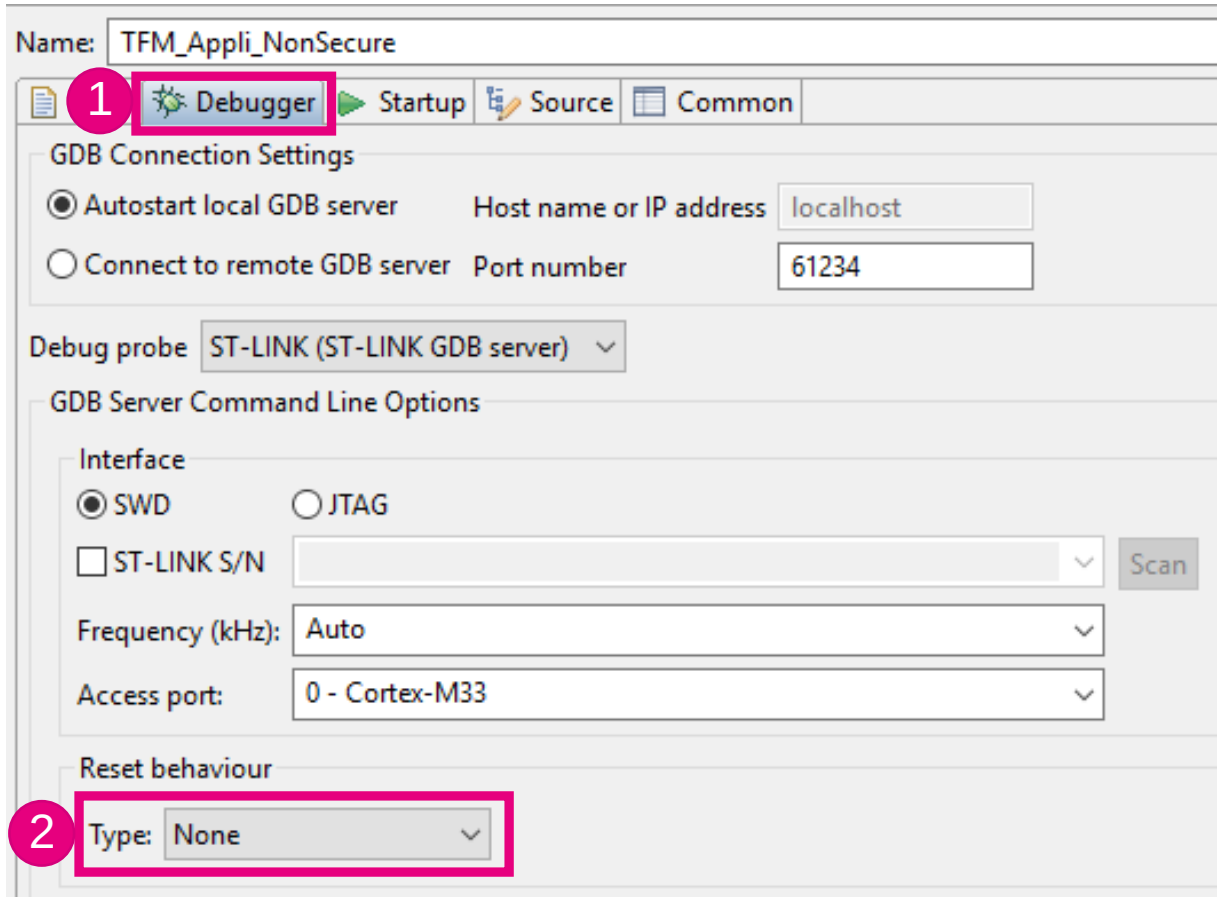
RDP 0.5 debug

- Please create the debug for Appli Non-secure and remove the reset and the download



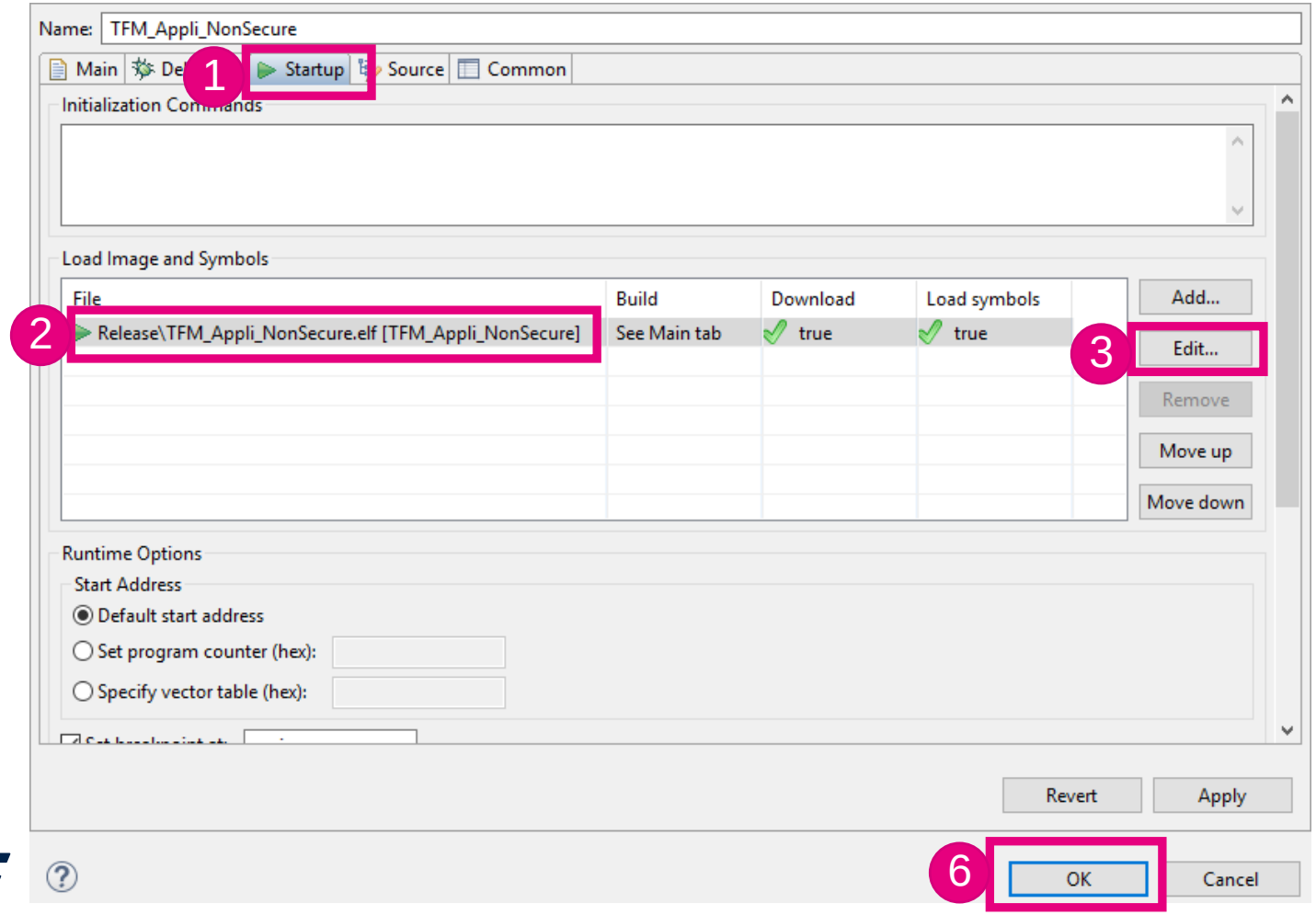
RDP 0.5 debug

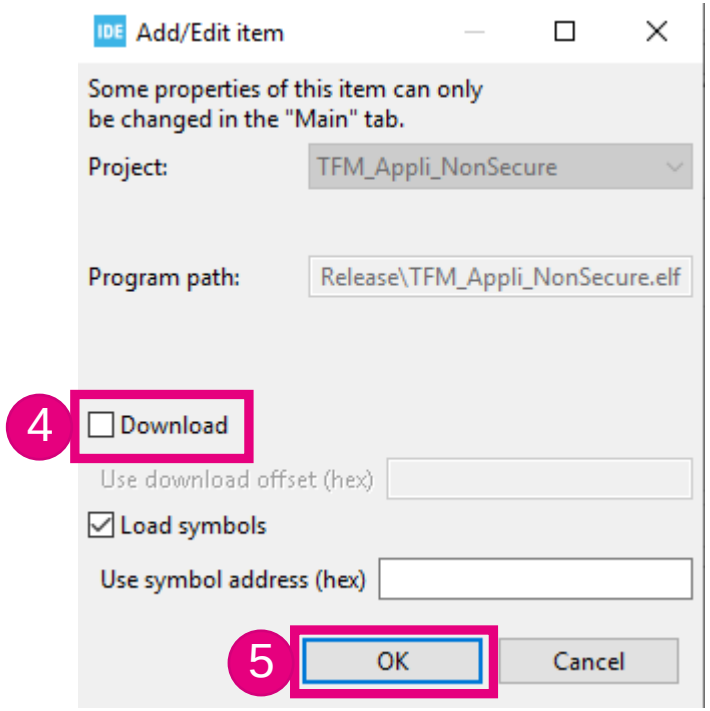
- Remove the reset at connection



RDP 0.5 debug

- Remove the download





RDP 0.5 debug

- Press the reset button, to stop at the entry point of the non-secure application

STM32SecuWS - TFM_Appli_NonSecure/Application/User/main.c - STM32CubeIDE

File Edit Source Refactor Navigate Search Project Run Window Help

Debug | Project Explorer

- TFM_Appli_NonSecure [STM32 Cortex-M C/C++
  - TFM_Appli_NonSecure.elf [cores: 0]
    - Thread #1 [main] 1 [core: 0] (Suspended : E
      - main() at main.c:121 0x8038ff8
  - arm-none-eabi-gdb (8.1.0.20180315)
  - ST-LINK (ST-LINK GDB server)

stm32l5xx_hal_uart.c | startup_stm32l5xx_ns.S | main.c

```
109     /* Return character written */
110     return ch;
111 }
112 #endif /*  __GNUC__ */
113
114 /**
115   * @brief  Main program
116   * @param  None
117   * @retval None
118   */
119 int main(int argc, char **argv)
120 /*int main(void) */
121 {
122   /*  set example to const : this const changes in binary without rebuild */
123   pUserAppId = (uint8_t *)&UserAppId;
124
125   /* STM32L5xx HAL library initialization:
126   - Systick timer is configured by default as source of time base, but user
127   can eventually implement his proper time base source (a general purpose
128   timer for example or other time source), keeping in mind that Time base
129   duration should be kept 1ms since PPP_TIMEOUT_VALUEs are defined and
130   handled in milliseconds basis.
```

Console | Problems | Executables | Debugger Console | Memory

Monitors: 0x0C001000

0x0C001000 : 0xC001000 <Hex> | New Renderings...

Address	0 - 3	4 - 7	8 - B	C - F
0C001000	????????	????????	????????	????????
0C001010	????????	????????	????????	????????
0C001020	????????	????????	????????	????????
0C001030	????????	????????	????????	????????

life.augmented

STM32CubeIDE debugging

- Terminate debugging session  or CTRL+F2

life.augmented

Remove TrustZone and protection!

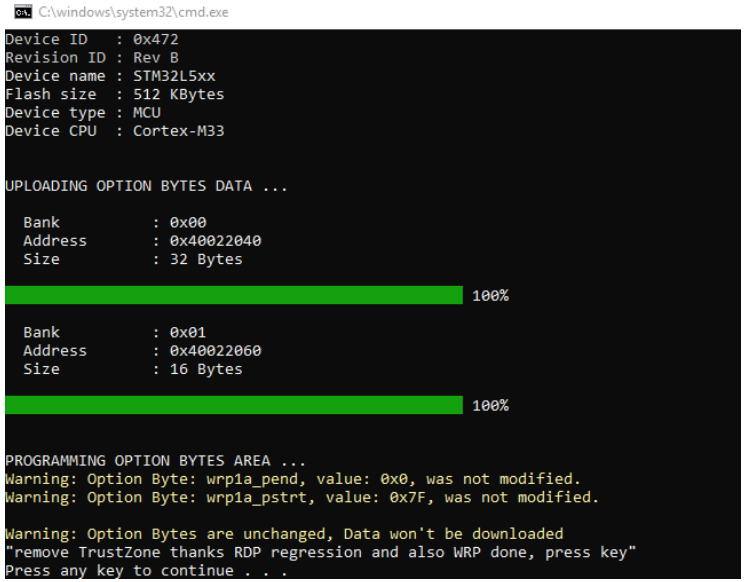
- We must do a RDP regression and TZEN = 0:

  RDP = 0x55 and TZEN = 0 -> flash full mass erase

  Remove WRP protection

C:\STM32SecuWS\TFM\Scripts

- To put your board in the init configuration please use :
  - STEP9_remove_TrustZone.bat



life.augmented

Finished !

During this hands-on, we have learned how to

- Compile and Debug the TFM on STM32L5
- Activate and use the HDP protection in the TFM context
- Debug a non-secure application with RDP level 0.5

life.augmented

Board clean up!

life.augmented

Board clean up!

C:\STM32SecuWS\TFM\Scripts

To clean up your board please use :

- STEP10_Prog_basic_app.bat

  -> activate TrustZone and flash a secure and a non-secure application (blue/green led blinking)

  WARNING this script should be ok (blue/green led blinking) before continue !!!

- STEP11_Regression.bat

  ->will activate RDP 0.5 then do a regression and deactivate TrustZone

Board clean up!

C:\windows\system32\cmd.exe

```
OPTION BYTES BANK: 0

   Read Out Protection:

     RDP          : 0xAA (Level 0, no protection)

   BOR Level:

     BOR_LEV      : 0x0 (BOR Level 0, reset level threshold is around 1.7 V)

   User Configuration:

     nRST_STOP    : 0x1 (No reset generated when entering Stop mode)
     nRST_STDBY   : 0x1 (No reset generated when entering Standby mode)
     nRST_SHDW    : 0x1 (No reset generated when entering the Shutdown mode)
     IWDG_SW      : 0x1 (Software independant watchdog)
     IWDG_STOP    : 0x1 (IWDG counter active in stop mode)
     IWDG_STDBY   : 0x1 (IWDG counter active in standby mode)
     WWDG_SW      : 0x1 (Software window watchdog)
     SWAP_BANK    : 0x0 (Bank 1 and bank 2 address are not swapped)
     DB256        : 0x1 (256Kb dual-bank Flash with contiguous addresses)
     DBANK        : 0x1 (Dual bank mode with 64 bits data)
     SRAM2_PE     : 0x1 (SRAM2 parity check disable)
     SRAM2_RST    : 0x0 (SRAM2 erased when a system reset occurs)
     nSWBOOT0     : 0x1 (BOOT0 taken from PH3/BOOT0 pin)
     nBOOT0       : 0x1 (nBOOT0 = 1)
     PA15_PUPEN   : 0x1 (USB power delivery dead battery disabled/ TDI pull-up activated)
     TZEN         : 0x0 (Global TrustZone security disabled)
     NSBOOTADD0   : 0x100000  (0x8000000)
     NSBOOTADD1   : 0x17F200  (0xBF90000)
     SECBOOTADD0  : 0x0  (0x0)
     BOOT_LOCK    : 0x0 (Boot based on the pad/option bit configuration)

   Write Protection 1:

     WRP1A_PSTRT  : 0x7F  (0x803F800)
     WRP1A_PEND   : 0x0  (0x8000000)
     WRP1B_PSTRT  : 0x7F  (0x803F800)
     WRP1B_PEND   : 0x0  (0x8000000)
OPTION BYTES BANK: 1

   Write Protection 2:

     WRP2A_PSTRT  : 0x7F  (0x807F800)
     WRP2A_PEND   : 0x0  (0x8040000)
     WRP2B_PSTRT  : 0x7F  (0x807F800)
     WRP2B_PEND   : 0x0  (0x8040000)
Press any key to continue . . .
```

life.augmented

Thank you

life.augmented

Recovery process…

If you don’t manage to connect with STM32CubeProgrammer.

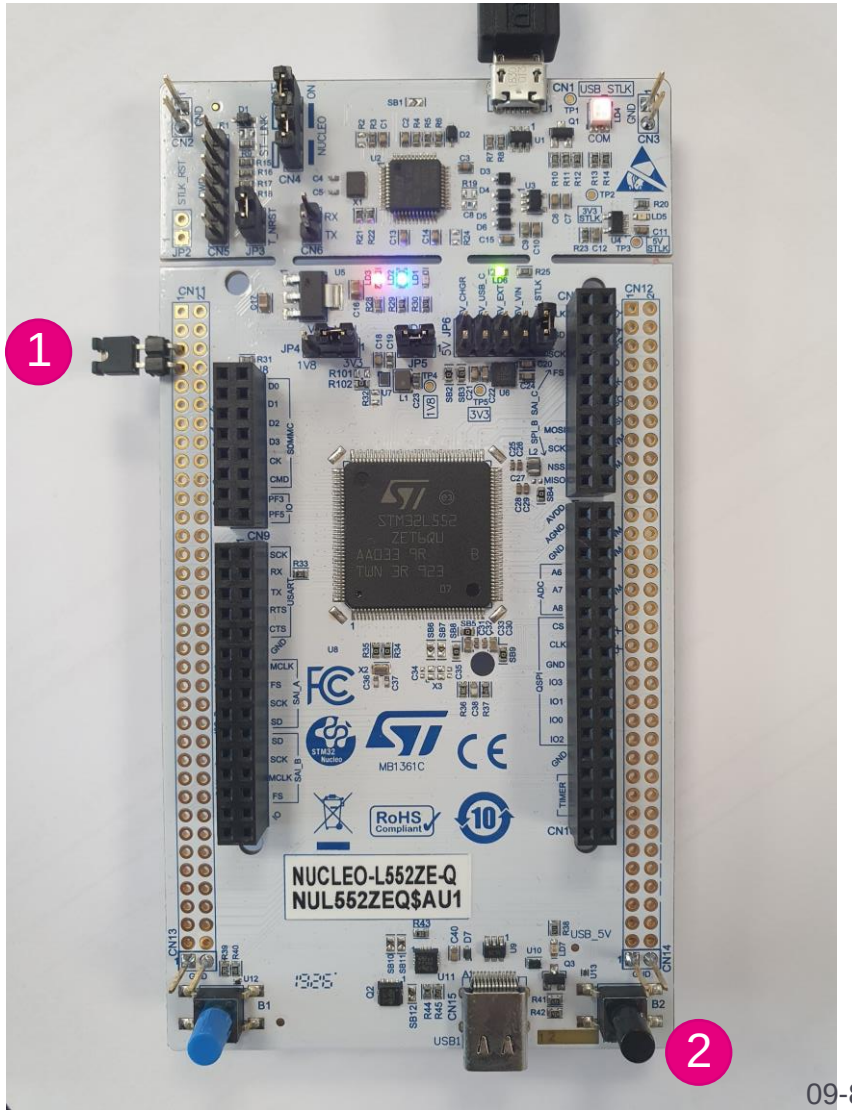
- To activate embedded bootloader, connect CN11 pin 5 and 7 then Reset.
- Blue led and red led should be on
- Then you can connect with CubeProgrammer (Hot Plug) and doing a regression with TrustZone remove.

  Option byte

  RDP = AA

  TZEN unchecked

  Apply



Appendix : STM32SecuWS\TFM\Scripts

- Purpose of the scripts:

Avoid any **mistake** in the setting of **option byte or binary programming** with STM32CubeProgrammer.

- Dependencies :

All the script use the command line interface of **Cube programmer**

STM32CubeProgrammer\bin\STM32_Programmer_CLI.exe

The path for this binary is set in the script :

STM32SecuWS\Tools\Other\SetEnv.bat

Script variable : stm32programmercli

life.augmented

Appendix

- STEP1_prepare_L5_for_TFM.bat :

  Flash mass erase

  Set option byte : TZEN=1, SRAM2_RST=0,vSECBOOTADD0=0x180032, DBANK=1 , SECWM1_PSTRT=0 , SECWM1_PEND=111

- STEP2_flash_precompiled_TFM.bat

  Flash: Archive\tfm_ns_sign.bin, Archive\tfm_s_sign.bin, Archive\TFM_SBSFU_Boot.bin

- STEP3_flash_mass_erase.bat

  Mass erase

- STEP4_flash_ns_binary.bat

  Flash: Binary tfm_ns_sign.bin

- STEP5_flash_s_binary.bat

  Flash: Binary tfm_s_sign.bin

- STEP6_flash_SBSFU_binary.bat

  Flash: Binary TFM_SBSFU_Boot.bin

life.augmented

Appendix

- STEP7_configure_HDP.bat

  Set option byte : HDP1_PEND=0x1C HDP1EN=0x1

- STEP8_activate_RDP_0_5.bat

  Set option byte : RDP=0x55

- STEP9_remove_TrustZone.bat

  Set option byte : TZEN=0, RDP=0xAA, WRP1A_PSTRT=0x7f, WRP1A_PEND=0

- STEP10_prog_basic_app.bat

  Set option byte : TZEN=1, SECBOOTADD0=0x180000, SECWM1_PSTRT=0,SECWM1_PEND=0x7F

  Do a mass erase

  Flash Regression\Nucleo\Project_ns.hex and Regression\Nucleo\Project_s.hex

- STEP11_regression.bat

  Set option byte : RDP=0x55

  Set option byte : TZEN=0, RDP=0xAA

  Display all option byte

life.augmented