



life.augmented

# **STM32 security workshop**

## **02 Building the SBSFU**

# Purpose

- Starting from the SBSFU build and execution on target
- We'll exercise the secure boot which will authenticate and launch an application
- Then we will generate a version 2 of the application and use the SBSFU to update it on the target

# Restarting from homework configuration

- During homework you have build 3 projects and generated 2 binaries
- You have flashed the binary containing both SBSFU and UserApp to the target
- Then you have been able to see the trace of execution of SBSFU and UserApp on TeraTerm
- Let's restart from this point
  - Please plug your Nucleo L476 containing the SBSFU and UserApp to your PC
  - Open an explorer window and go to C:\STM32SecuWS\L4\Scripts
  - Launch 00\_StartTeraTermL4
  - Press reset button

# Quick view on traces after reset

```
COM60 - Tera Term VT
File Edit Setup Control Window Help

= [ISBOOT] System Security Check successfully passed. Starting...
=====
=          <C> COPYRIGHT 2017 STMicroelectronics
=          Secure Boot and Secure Firmware Update
=====

= [ISBOOT] SECURE ENGINE INITIALIZATION SUCCESSFUL
= [ISBOOT] STATE: CHECK STATUS ON RESET
=          INFO: A Reboot has been triggered by a Hardware reset!
=          INFO: Last execution detected error was: No error. Success.
= [ISBOOT] STATE: CHECK NEW FIRMWARE TO DOWNLOAD
= [ISBOOT] STATE: CHECK USER FW STATUS
=          A FW is detected in the slot SLOT_ACTIVE_1
= [ISBOOT] STATE: VERIFY USER FW SIGNATURE
= [ISBOOT] STATE: EXECUTE USER FIRMWARE
=====
=          <C> COPYRIGHT 2017 STMicroelectronics
=          User App #A
=====

===== Main Menu =====
Download a new Fw Image ----- 1
Test Protections ----- 2
Test SE User Code ----- 3
Multiple download ----- 4
Validate a FW Image ----- 5
Selection :
```

Check security  
protections and  
setup consistency

Initialise the secure  
engine

Boot status check

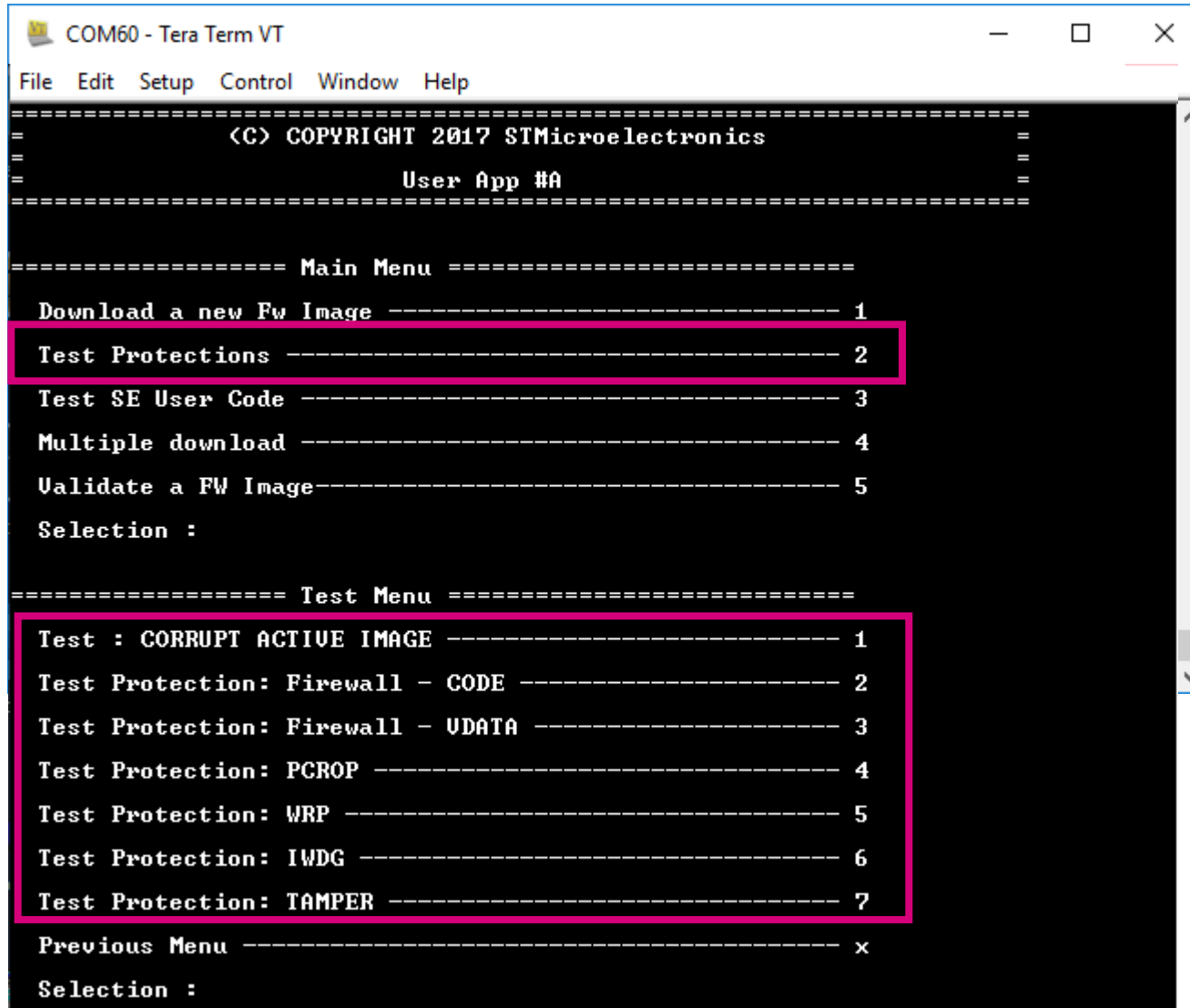
Check local update request

Check fw status: Download slot to  
install, interrupted installation,  
Active firmware presence...

Verify Active fw signature

Verify active fw signature  
(second time) and launch  
application

# Test protection menu



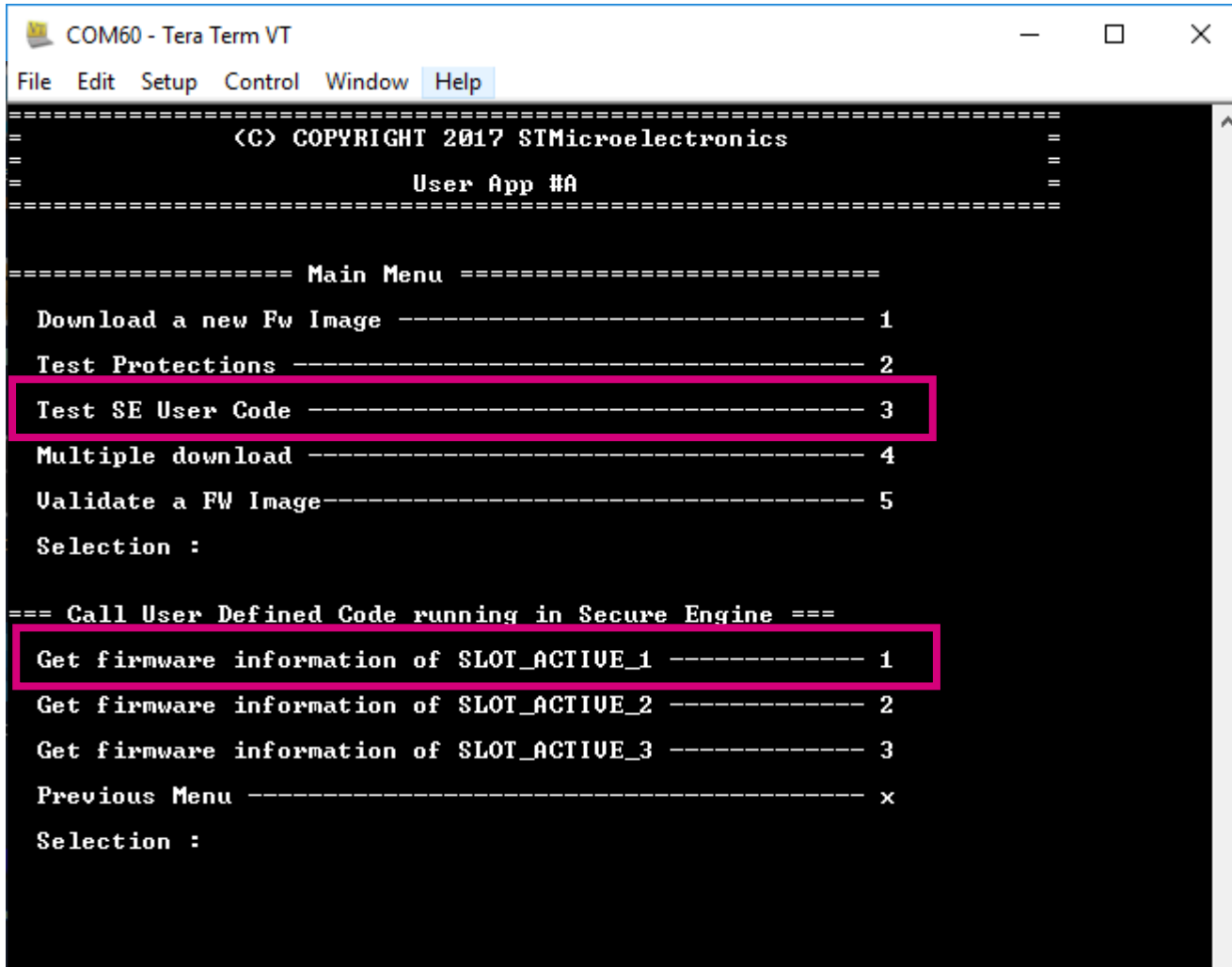
```
COM60 - Tera Term VT
File Edit Setup Control Window Help
=====
(C) COPYRIGHT 2017 STMicroelectronics
=====
User App #A
=====

===== Main Menu =====
Download a new Fw Image ----- 1
Test Protections ----- 2
Test SE User Code ----- 3
Multiple download ----- 4
Validate a FW Image ----- 5
Selection :

===== Test Menu =====
Test : CORRUPT ACTIVE IMAGE ----- 1
Test Protection: Firewall - CODE ----- 2
Test Protection: Firewall - UDATA ----- 3
Test Protection: PCROP ----- 4
Test Protection: WRP ----- 5
Test Protection: IWDG ----- 6
Test Protection: TAMPER ----- 7
Previous Menu ----- x
Selection :
```

- Press 2
- Then you can play with these options to see what happens
- If you corrupt the image in SLOT\_ACTIVE\_1 you will have to launch the scripts **00\_ResetL4Target** and **01\_Flash\_SBSFU\_UserApp**

# Test SE User Code menu



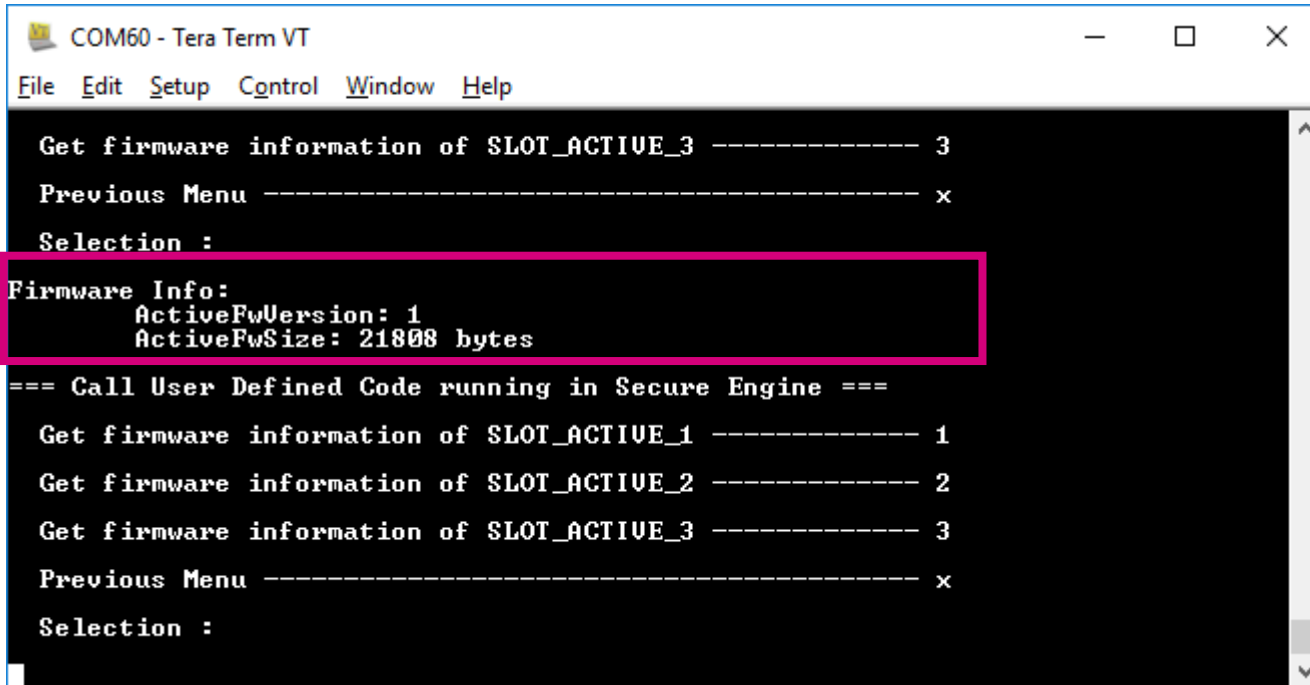
```
COM60 - Tera Term VT
File Edit Setup Control Window Help
=====
<C> COPYRIGHT 2017 STMicroelectronics
=====
User App #A
=====

===== Main Menu =====
Download a new Fw Image ----- 1
Test Protections ----- 2
Test SE User Code ----- 3
Multiple download ----- 4
Validate a FW Image ----- 5
Selection :

=== Call User Defined Code running in Secure Engine ===
Get firmware information of SLOT_ACTIVE_1 ----- 1
Get firmware information of SLOT_ACTIVE_2 ----- 2
Get firmware information of SLOT_ACTIVE_3 ----- 3
Previous Menu ----- x
Selection :
```

- Press 3 and then 1

# Test SE User Code menu



The screenshot shows a terminal window titled "COM60 - Tera Term VT". The menu displayed is as follows:

```
Get firmware information of SLOT_ACTIVE_3 ----- 3
Previous Menu ----- x
Selection :
Firmware Info:
  ActiveFwVersion: 1
  ActiveFwSize: 21808 bytes
=== Call User Defined Code running in Secure Engine ===
Get firmware information of SLOT_ACTIVE_1 ----- 1
Get firmware information of SLOT_ACTIVE_2 ----- 2
Get firmware information of SLOT_ACTIVE_3 ----- 3
Previous Menu ----- x
Selection :
```

The "Firmware Info:" section is highlighted with a red box.

- It shows information available from application side

# Note about active slots

- Active slot is where active user firmware is located
- By opposition with download slot where new version of the firmware is downloaded
- There are 3 possible active and download slots managed by SBSFU
- The main purpose of having more than one active slot is the support of multiple cores chips with independent firmware.



# SBSFU in a nutshell

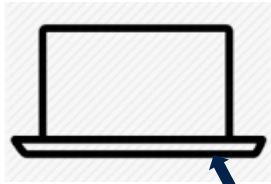
- You should now have a first view on:
  - SBSFU directory structure
  - How to build the SBSFU : Need to be done in order
  - SBSFU generates useful files for download in UserApp/binary directory
  - SBSFU + User application are loaded at the same time on the target
  - SBSFU is activating secure protections
  - SBSFU checks the user application authenticity and launches it
  - Default User application provides some basic menu allowing
    - To check some protections
    - To call a SBSFU API
    - To perform an update
- Let's see how update is working

# Firmware update

- First menu launches a firmware update
- This update is managed inside the application
- Application will receive the firmware through Ymodem protocol
- Then it will write each chunk in a spare part of the flash.
- At the end, the application should reset the chip to launch the secure boot
- Secure boot will detect this new firmware and install it

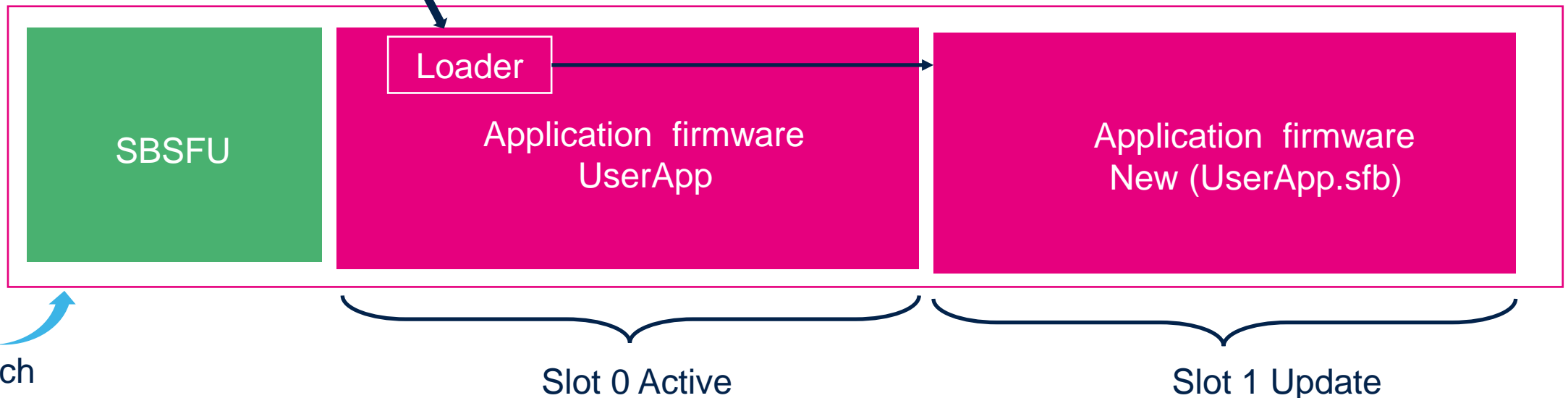
# Firmware update principle

TeraTerm



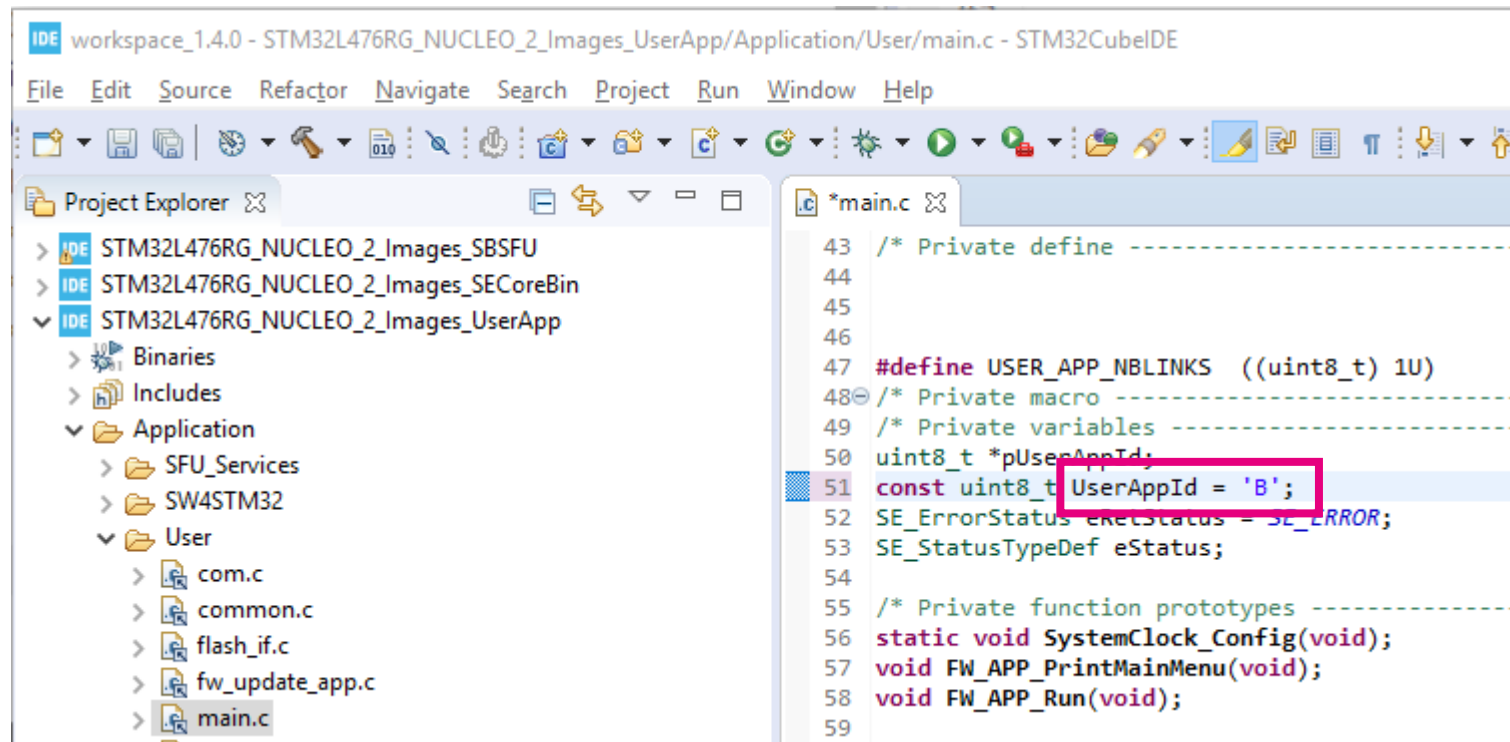
Ymodem

- Transfer update firmware
- Reset : secure boot detects new fw
- Secure boot checks new firmware
- Secure boot install new firmware



# Prepare an update image

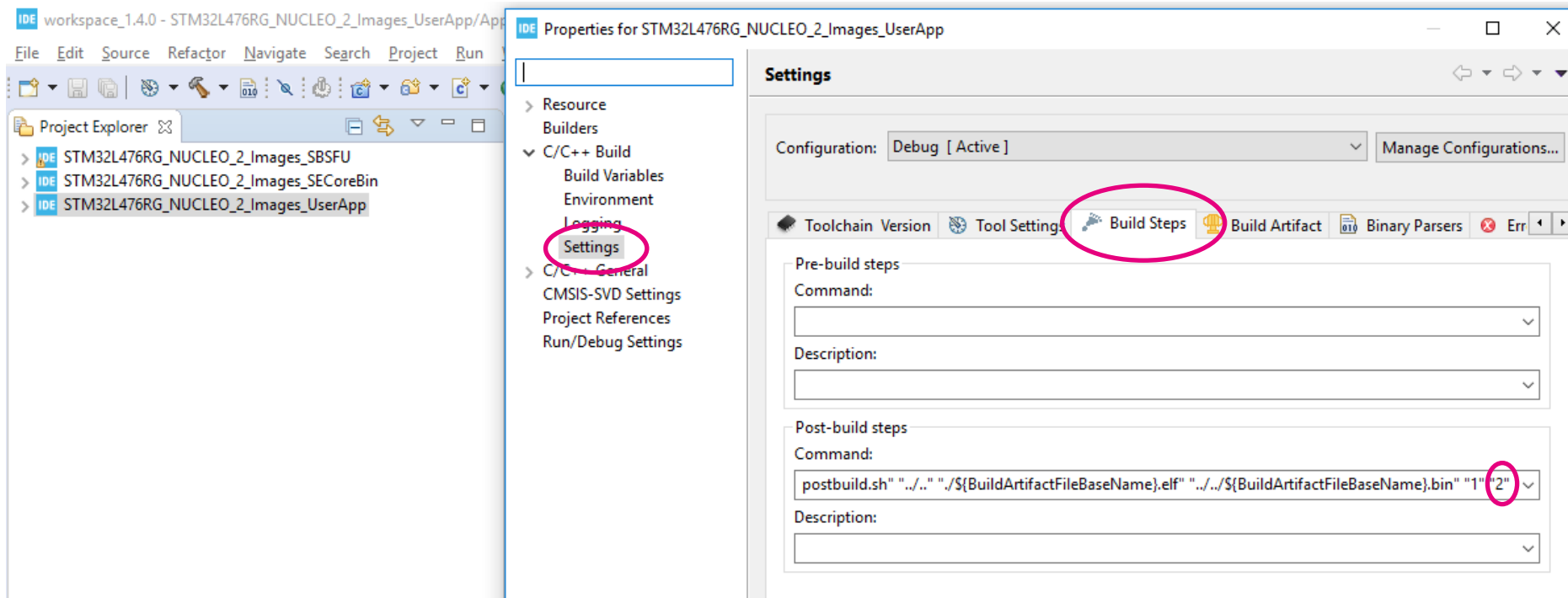
- Open same workspace in STM32CubeIDE you've used for the homework
- Change the application identifier in the code :



```
workspace_1.4.0 - STM32L476RG_NUCLEO_2_Images_UserApp/Application/User/main.c - STM32CubeIDE
File Edit Source Refactor Navigate Search Project Run Window Help
Project Explorer
  > IDE STM32L476RG_NUCLEO_2_Images_SBSFU
  > IDE STM32L476RG_NUCLEO_2_Images_SECoreBin
  > IDE STM32L476RG_NUCLEO_2_Images_UserApp
    > Binaries
    > Includes
    > Application
      > SFU_Services
      > SW4STM32
      > User
        > com.c
        > common.c
        > flash_if.c
        > fw_update_app.c
        > main.c
main.c
43 /* Private define -----
44
45
46
47 #define USER_APP_NBLINKS ((uint8_t) 1U)
48 /* Private macro -----
49 /* Private variables -----
50 uint8_t *pUserAppId;
51 const uint8_t UserAppId = 'B';
52 SE_ErrorStatus eKetStatus = SE_ERROR;
53 SE_StatusTypeDef eStatus;
54
55 /* Private function prototypes -----
56 static void SystemClock_Config(void);
57 void FW_APP_PrintMainMenu(void);
58 void FW_APP_Run(void);
59
```

# Update: prepare image

- Change the version of the UserApp
  - Click on STM32L476RG\_NUCLEO\_2\_Images\_UserApp, click on menu Project/Properties
  - Goto C++Build/Settings/BuildSteps
  - Edit post build steps replace the last “1” by “2”, apply and close



# Update: compile new version

- Launch build  on UserApp project to generate version 2

```
CDT Build Console [STM32L476RG_NUCLEO_2_Images_UserApp]
arm-none-eabi-gcc -z max-page-size=1 -o "UserApp.elf" @"objects.list" -l:se_interface_app.o -mcpu=cortex-m4 -T"../STM3
Finished building target: UserApp.elf

arm-none-eabi-size UserApp.elf
  text    data    bss     dec     hex filename
 21632    176    6000    27808    6ca0 UserApp.elf
Finished building: default.size.stdout

arm-none-eabi-objdump -h -S UserApp.elf > "UserApp.list"
Finished building: UserApp.list

arm-none-eabi-objcopy -O binary UserApp.elf "UserApp.bin"
Finished building: UserApp.bin

arm-none-eabi-objcopy -O binary "UserApp.elf" "../../UserApp.bin"
arm-none-eabi-size "UserApp.elf"
  text    data    bss     dec     hex filename
 21632    176    6000    27808    6ca0 UserApp.elf
"../../../../../2_Images_SECoreBin/SW4STM32/postbuild.sh" "../../" "../UserApp.elf" "../../UserApp.bin" "1" "2"
prepareimage with windows executable

17:39:10 Build Finished. 0 errors, 0 warnings. (took 15s.896ms)
```

# Update: trigger update on target

In TeraTerm Press 1 to select the Download of a new Fw Image

```
===== Main Menu =====
Download a new Fw Image ----- 1
Test Protections ----- 2
Test SE User Code ----- 3
Selection :

===== New Fw Download =====
-- Send Firmware
-- -- Erasing download area ...
-- -- File> Transfer> YMODEM> Send .....
```

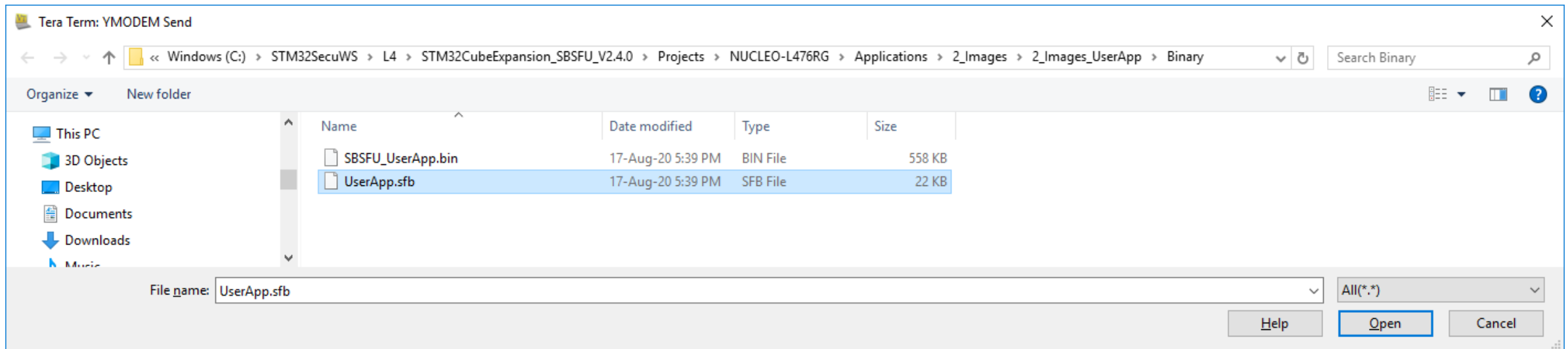
Wait for Ymodem request on the screen,  
and select File/Transfer/YMODEM/Send

The screenshot shows the TeraTerm VT window titled 'COM60 - Tera Term VT'. The 'File' menu is open, showing options like 'New connection...', 'Duplicate session', 'Cygwin connection', 'Log...', 'Comment to Log...', 'View Log', 'Show Log dialog...', 'Send file...', 'Transfer', 'Change directory...', 'Replay Log...', 'Print...', 'Disconnect', 'Exit', and 'Exit All'. The 'Transfer' option is highlighted, and its submenu is open, showing 'Kermit', 'XMODEM', 'YMODEM', 'ZMODEM', 'B-Plus', and 'Quick-VAN'. The 'YMODEM' option is highlighted, and its submenu is open, showing 'Receive...' and 'Send...'. The 'Send...' option is highlighted. In the background, the terminal text shows a successful firmware update: 'S ON RESET', 'been triggered by a Hardware reset!', 'on detected error was: No error. Success.', 'FIRMWARE TO DOWNLOAD', 'FW STATUS', 'n the slot SLOT\_ACTIVE\_1', 'FW SIGNATURE', 'R FIRMWARE', '=====', '2017 STMicroelectronics', 'ser App #A', '====='. Below the menu, the terminal text shows the 'New Fw Download' menu: '===== New Fw Download =====', '-- Send Firmware', '-- -- Erasing download area ...', '-- -- File> Transfer> YMODEM> Send ..'.

# Update: select update file

Popup window should display by default the directory in SBSFU  
C:\STM32SecuWS\L4\STM32CubeExpansion\_SBSFU\_V2.4.0\Projects\NUCLEO-L476RG\Applications\2\_Images\2\_Images\_UserApp\Binary

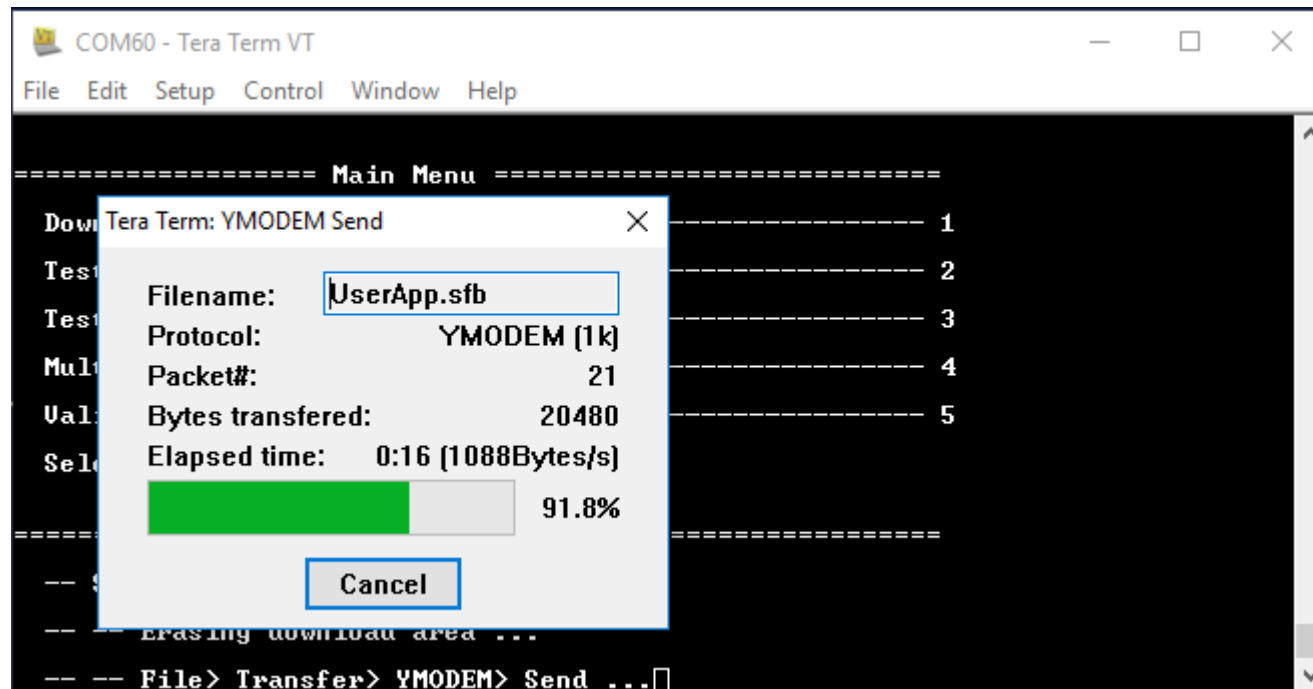
Select UserApp.sfb





# Update: download

New firmware transfer



# Update process

```
COM60 - Tera Term VT
File Edit Setup Control Window Help

===== New Fw Download =====
-- Send Firmware
-- -- Erasing download area ...
-- -- File> Transfer> YMODEM> Send ...
-- -- Programming Completed Successfully!
-- -- Bytes: 22320
-- Image correctly downloaded - reboot

= [ISBOOT] System Security Check successfully passed. Starting...

=====
=          <C> COPYRIGHT 2017 STMicroelectronics          =
=====
Secure Boot and Secure Firmware Update
=====

= [ISBOOT] SECURE ENGINE INITIALIZATION SUCCESSFUL
= [ISBOOT] STATE: CHECK STATUS ON RESET
INFO: A Reboot has been triggered by a Software reset!
INFO: Last execution detected error was: No error. Success.
= [ISBOOT] STATE: CHECK NEW FIRMWARE TO DOWNLOAD
= [ISBOOT] STATE: CHECK USER FW STATUS
New Fw to be installed from slot SLOT_DWL_1
= [ISBOOT] STATE: INSTALL NEW USER FIRMWARE
Image preparation done.
Swapping the firmware images.....

===== End of Execution =====

= [ISBOOT] System Security Check successfully passed. Starting...

=====
=          <C> COPYRIGHT 2017 STMicroelectronics          =
=====
Secure Boot and Secure Firmware Update
=====
```

Application manages the full download and then reset to activate the secureboot

New firmware detected in SLOT\_DWL\_1 to be installed. Verify new header signature

Firmware installation: Check version, Decryption in place, check fw signature, SWAP

Reset.

```
COM60 - Tera Term VT
File Edit Setup Control Window Help

= [SBOOT] SECURE ENGINE INITIALIZATION SUCCESSFUL
= [SBOOT] STATE: CHECK STATUS ON RESET
      INFO: A Reboot has been triggered by a Software reset!
      INFO: Last execution detected error was: No error. Success.
= [SBOOT] STATE: CHECK NEW FIRMWARE TO DOWNLOAD
= [SBOOT] STATE: CHECK USER FW STATUS
      A FW is detected in the slot SLOT_ACTIVE_1
= [SBOOT] STATE: VERIFY USER FW SIGNATURE
= [SBOOT] STATE: EXECUTE USER FIRMWARE
=====
      (C) COPYRIGHT 2017 STMicroelectronics
=====
      User App #B
=====

===== Main Menu =====
Download a new Fw Image ----- 1
Test Protections ----- 2
Test SE User Code ----- 3
Multiple download ----- 4
Validate a FW Image----- 5
Selection :

=== Call User Defined Code running in Secure Engine ===
Get firmware information of SLOT_ACTIVE_1 ----- 1
Get firmware information of SLOT_ACTIVE_2 ----- 2
Get firmware information of SLOT_ACTIVE_3 ----- 3
Previous Menu ----- x
Selection :

Firmware Info:
  ActiveFwVersion: 2
  ActiveFwSize: 21808 bytes
```

# Update: check version

- Check new version using the Test SE User Code menu

- SBSFU build is simple
- SBSFU is a secure bootloader that checks integrity and authenticity of the application
- SBSFU is able to securely update the application, checking integrity and authenticity at each step
- Update application transfer uses Ymodem protocol

# Thank you