Secure Boot on a SX350X or SX550X Switch

Objective

The purpose of this article is to explain the process of Secure Boot, a method to boot up with only trusted software. This feature is enabled starting with firmware version 2.4.0.91.

If you are unfamiliar with the terms used below, check out Cisco Business: Glossary of New Terms .

Applicable Devices

- SX350X
- SX550X

Software Version

- 2.4.0.91

Introduction

Secure Boot is a way of loading and running a secure image using a chain-of-trust to avoid loading untrusted software. A chain-of- trust is established by assigning images with private keys and using hardware and software mechanisms to verify the loaded image. This allows users to be sure that when they load device firmware, no other person has added a security violating code.

When a user tries to load a new image, the new image is downloaded to a temporary file, which is validated. In case of error, the temporary file is deleted. This way, if the new image is not valid, the installation process will fail and show a warning message.

If your Switches are in a Stacked Topology

When you load 2.4.0.91, or the latest version available, onto the active (primary) switch, it will load the firmware on all the members of the stack. This is regardless of the model within the family, as it is a requirement that all the devices run the same firmware. The stack will function normally.

Secure Boot Process

During bootup, the system will print Secure Boot information on the terminal. Here are the steps the devices check through before the Secure Boot.

- *Boot Read Only Memory (BootROM)* validates *booton*

Booton validates Universal Boot (*Uboot)*

Uboot validates the *ROS image*

If the Secure Boot detects failure, it will prevent the device from booting up. If this occurs, contact your Cisco Partner or Technical Assistance Center (TAC) to determine the next steps to follow in this situation. If you need to find a Cisco Partner, click here.

Secure Boot Syslog

During bootup, the system will print Secure Boot information:

Secure Boot enabled/disabled – in devices with no System-on-Chip (SoC) electrical programmable fuse (eFuse), such as Minimal SYStem (MSYS) Central Processing Unit (CPU), or when eFuse secure bit is not set, the printout will be “Secure Boot disabled”. If Secure Boot is enabled, the printout will be “Secure Boot enabled”.

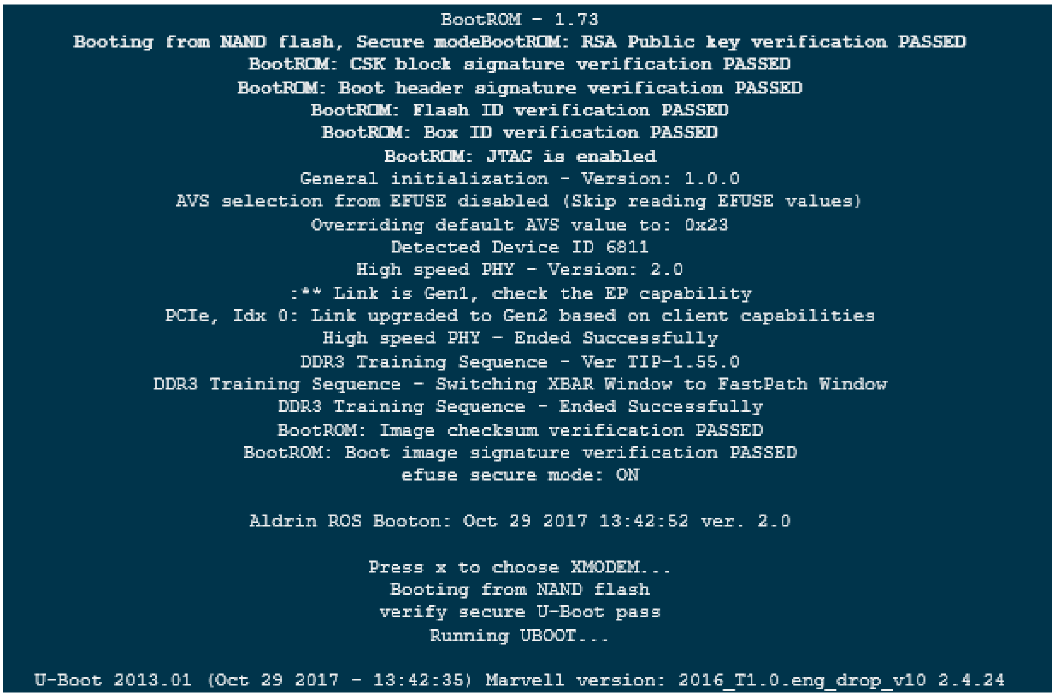
After *BootROM* validates the *booton*, it prints the validation status (*passed/failed*).

After *booton* validates the *Uboot*, it prints the validation status (*passed/failed*).

After *Uboot* validates the *ros image*, it prints the validation status (*passed/failed*).

Note: In case of failure, the boot process will stop.

Secure Boot output example firmware version 2.4.0.91:



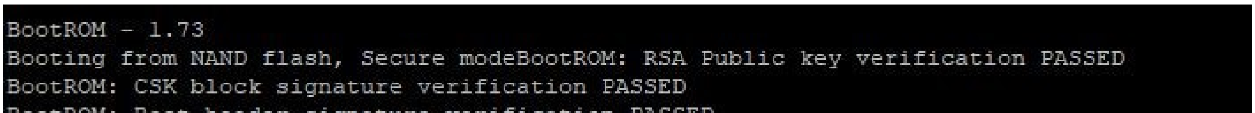
```
BootROM - 1.73
Booting from NAND flash, Secure modeBootROM: RSA Public key verification PASSED
BootROM: CSK block signature verification PASSED
BootROM: Boot header signature verification PASSED
BootROM: Flash ID verification PASSED
BootROM: Box ID verification PASSED
BootROM: JTAG is enabled
General initialization - Version: 1.0.0
AVS selection from EFUSE disabled (Skip reading EFUSE values)
Overriding default AVS value to: 0x23
Detected Device ID 6811
High speed PHY - Version: 2.0
:** Link is Gen1, check the EP capability
PCIe, Idx 0: Link upgraded to Gen2 based on client capabilities
High speed PHY - Ended Successfully
DDR3 Training Sequence - Ver TIP-1.55.0
DDR3 Training Sequence - Switching XBAR Window to FastPath Window
DDR3 Training Sequence - Ended Successfully
BootROM: Image checksum verification PASSED
BootROM: Boot image signature verification PASSED
efuse secure mode: ON

Aldrin ROS Booton: Oct 29 2017 13:42:52 ver. 2.0

Press x to choose XMODEM...
Booting from NAND flash
verify secure U-Boot pass
Running UBOOT...

U-Boot 2013.01 (Oct 29 2017 - 13:42:35) Marvell version: 2016_T1.0.eng_drop_v10 2.4.24
```

Secure Boot output example firmware version 2.5.0.83:



```
BootROM - 1.73
Booting from NAND flash, Secure modeBootROM: RSA Public key verification PASSED
BootROM: CSK block signature verification PASSED
BootROM: Boot header signature verification PASSED
```

Conclusion

You are now familiar with Secure Boot and how it can help protect your network.