Inicialização segura em um switch SX350X ou SX550X

Objetivo

A finalidade deste artigo é explicar o processo do Secure Boot, um método de inicialização somente com software confiável. Esse recurso é ativado a partir do firmware versão 2.4.0.91.

Se você não está familiarizado com os termos usados abaixo, confira o Cisco Business: Glossário de Novos Termos.

Dispositivos aplicáveis

SX350X

SX550X

Versão de software

2.4.0.91

Introduction

O Secure Boot é uma forma de carregar e executar uma imagem segura usando uma cadeia de confiança para evitar carregar software não confiável. Uma cadeia de confiança é estabelecida pela atribuição de imagens com chaves privadas e pelo uso de mecanismos de hardware e software para verificar a imagem carregada. Isso permite que os usuários tenham certeza de que, quando carregam o firmware do dispositivo, nenhuma outra pessoa adicionou um código de violação de segurança.

Quando um usuário tenta carregar uma nova imagem, a nova imagem é baixada para um arquivo temporário, que é validado. Em caso de erro, o arquivo temporário é excluído. Dessa forma, se a nova imagem não for válida, o processo de instalação falhará e exibirá uma mensagem de aviso.

Se seus Switches estiverem em uma topologia empilhada

Quando você carregar 2.4.0.91, ou a versão mais recente disponível, no switch ativo (primário), ele carregará o firmware em todos os membros da pilha. Isso independentemente do modelo dentro da família, pois é um requisito que todos os dispositivos executem o mesmo firmware. A pilha funcionará normalmente.

Processo de inicialização segura

Durante a inicialização, o sistema imprimirá informações de inicialização segura no terminal. Aqui

estão as etapas pelas quais os dispositivos verificam antes do Secure Boot.

A memória de inicialização somente leitura (BootROM) valida a *inicialização*

A inicialização valida a inicialização universal (*inicialização)*

A inicialização valida a *imagem do ROS*

Se o Secure Boot detectar falha, ele impedirá que o dispositivo seja inicializado. Se isso ocorrer, entre em contato com o seu Parceiro da Cisco ou Centro de Assistência Técnica (TAC) para determinar as próximas etapas a serem seguidas nessa situação. Se precisar encontrar um parceiro da Cisco, clique aqui.

Syslog de inicialização segura

Durante a inicialização, o sistema imprimirá as informações de inicialização segura:

Secure Boot enabled/disabled - em dispositivos sem fusível programável elétrico (eFuse) do System-on-Chip (SoC), como Unidade Central de Processamento (CPU - Central Processing Unit) do Minimal SYStem (MSYS), ou quando o bit seguro do eFuse não estiver definido, a impressão será "Secure Boot disabled". Se o Secure Boot estiver habilitado, a impressão será "Secure Boot enabled" (Inicialização segura habilitada).

Depois que o *BootROM* valida a *inicialização*, ele imprime o status de validação (*passado/falha*).

Depois que a *inicialização* valida a *inicialização*, ele imprime o status de validação (*passado/falha*).

Depois que a *inicialização* valida a *imagem do ros*, ela imprime o status de validação (*passado/falha*).

Note: Em caso de falha, o processo de inicialização será interrompido.

Exemplo de firmware de saída de inicialização segura versão 2.4.0.91:

Exemplo de firmware de saída de inicialização segura versão 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
BootROM: Flash ID verification PASSED


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

Init Customer board mvHwsPexConfig: 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


Armada38x Booton: Apr 17 2018 21:23:48 ver. 2.1.3
efuse secure mode: ON

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


U-Boot 2013.01 (Jun 18 2019 - 16:47:25) Marvell version: 2016_T1.0.eng_drop_v10 2.5.18

Loading system/images/active-image ...
Verify ROS secure Image pass, efuse is programmed
Uncompressing Linux... done, booting the kernel.
I2C frequency 100 kHz (Tclk 200 MHz, freq_m 12, freq_n 3)
```

Conclusão

Agora você está familiarizado com o Secure Boot e como ele pode ajudar a proteger sua rede.