SX350XまたはSX550Xスイッチでのセキュアブート

目的

この記事の目的は、信頼できるソフトウェアだけで起動するセキュアブートのプロセスを説明することです。この機能は、ファームウェアバージョン2.4.0.91以降で有効になります。

次の用語に慣れていない場合は、シスコビジネスをご覧[ください。新用語一覧](#)。

該当するデバイス

SX350X

SX550X

[Software Version]

2.4.0.91

概要

セキュアブートは、信頼できないソフトウェアのロードを回避するために、信頼チェーンを使用してセキュアイメージをロードおよび実行する方法です。秘密鍵を使用してイメージを割り当て、ハードウェアおよびソフトウェアのメカニズムを使用してロードされたイメージを検証することにより、信頼の連鎖が確立されます。これにより、ユーザはデバイスファームウェアをロードするときに、他のユーザがセキュリティ違反コードを追加していないことを確認できます。

ユーザが新しいイメージをロードしようとすると、新しいイメージが一時ファイルにダウンロードされ、検証されます。エラーの場合、一時ファイルは削除されます。これにより、新しいイメージが有効でない場合、インストールプロセスが失敗し、警告メッセージが表示されます。

スイッチがスタック型トポロジの場合

アクティブ（プライマリ）スイッチに2.4.0.91または利用可能な最新バージョンをロードすると、スタックのすべてのメンバにファームウェアがロードされます。すべてのデバイスが同じファームウェアを実行することが要件であるため、これはファミリ内のモデルに関係ありません。スタックは正常に機能します。

セキュアブートプロセス

ブートアップ時に、システムはターミナルのセキュアブート情報を印刷します。デバイスがセキュアブートの前にチェックする手順を次に示します。

ブート読み取り専用メモリ(BootROM)によるブートオンの検証を行う

Bootonはユニバーサルブート(Uboot)を*有効にします。*

UbootはROSイメージを検証します

セキュアブートで障害が検出されると、デバイスの起動が妨げられます。この問題が発生した場合は、シスコパートナーまたはTechnical Assistance Center(TAC)にお問い合わせくださ*い。*この状況で次に行う手順を決定してください。シスコパートナーを検索する必要がある場合は、ここをクリックします。

セキュアブートSyslog

ブートアップ時に、システムはセキュアブート情報を出力します。

セキュアブートの有効/無効：システムオンチップ(SoC)電気プログラマブルヒューズ(eFuse)がないデバイス(Minimal SYStem (MSYS) Central Processing Unit (CPU)など)、またはeFuseセキュアビットが設定されていない場合、プリントアウトは「セキュアブート無効」になります。セキュアブートが有効になっている場合、印刷イメージは「セキュアブートが有効」になります。

BootROM*がブートオン*を検証*した*後、検証ステータスが表示されます(*成功/失敗*)。

ブートオン*が*Ubootを*検証*した後、検証ステータス(*成功/失敗)を表示*します。

Uboot*が rosイメージを検証*した後、検証ステータスを出力します(*成功/失敗*)。

注：障害が発生した場合、ブートプロセスは停止します。

セキュアブートの出力例ファームウェアバージョン2.4.0.91:

セキュアブートの出力例ファームウェアバージョン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)
```

結論

セキュアブートと、セキュアブートがネットワークの保護にどのように役立つかについて理解しています。