Android Verified Boot

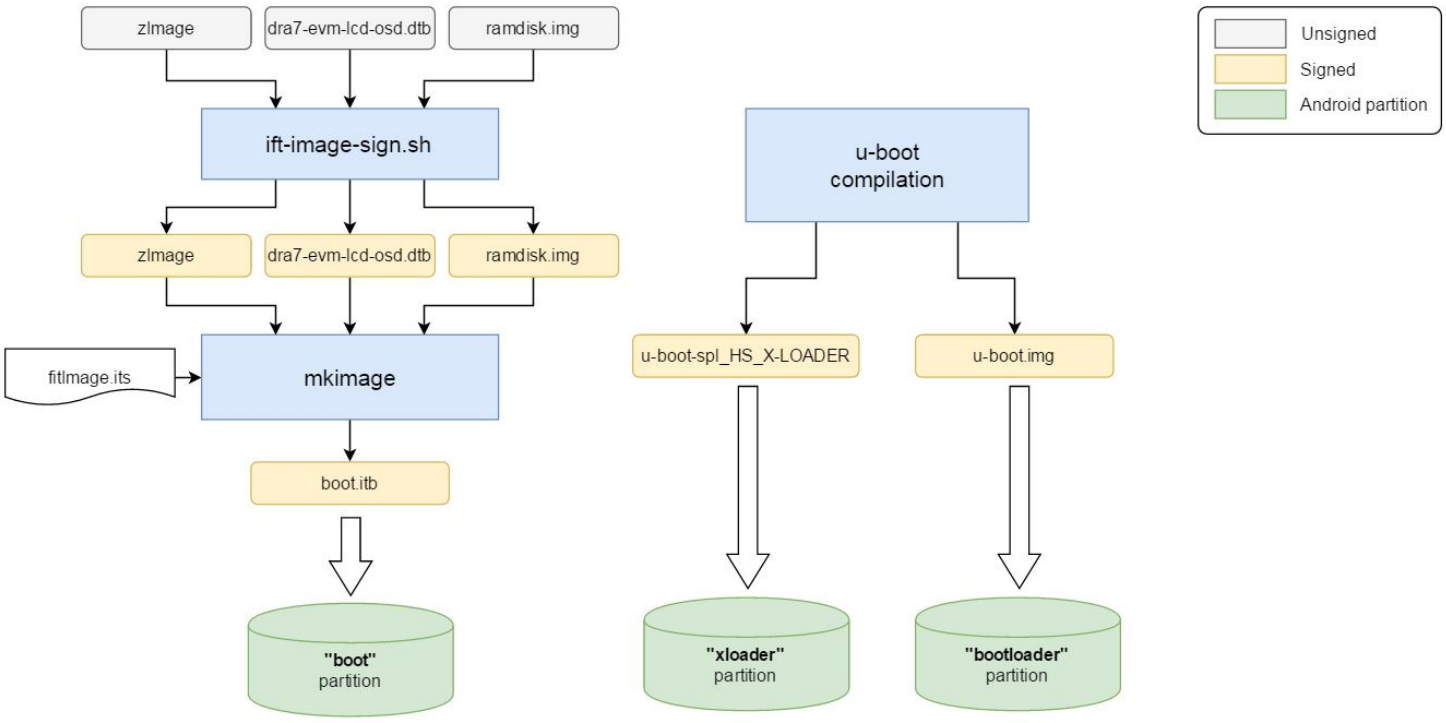
Contents

6AM.1.3 Release

Verified Boot in this release is being implemented with the TI Automotive SECDEV package for the verification of the kernel, device-tree blob and ramdisk. The Linux kernel device-mapper-verity feature is used for validation of Android system image. Please refer to Android documentation (https://source.android.com/security/verifiedboot/index.html) for further details on Verified Boot in Android.

Creating the boot image

The signing and creation of the FIT boot image is shown in the figure below.



Steps

1. Set the TI_SECURE_DEV_PKG environment variable to the directory where the TI SECDEV package has been installed

2. Compile the bootloaders for the DRA7xx HS device

```
cd ${UBOOT}
export CROSS_COMPILE=${MYDROID}/prebuilts/gcc/linux-x86/arm/arm-linux-androideabi-4.9/bin/arm-linux-androideabi-
export ARCH=arm
make distclean
make dra7xx_hs_evm_config
make
```

3. Compile the Android kernel, refer to the release notes for instructions

4. Compile the Android filesystem, refer to the release notes for instructions

5. Create a work directory

```
mkdir work
cd work
mkdir -p signed/dtb
```

6. Copy the bootloader, kernel, dtbs and ramdisk images to the work directory

```
cp ${UBOOT}/u-boot-spl_HS_X-LOADER .
cp ${UBOOT}/u-boot.img .
cp ${MYDROID}/out/target/product/jacinto6evm/ramdisk.img .
cp ${KERNEL}/arch/arm/boot/zImage .
cp ${KERNEL}/arch/arm/boot/dts/dra7*.dtb .
```

7. Sign the ramdisk, kernel and dtb files

```
${TI_SECURE_DEV_PKG}/scripts/ift-image-sign.sh dra7xx zImage signed/zImage
${TI_SECURE_DEV_PKG}/scripts/ift-image-sign.sh dra7xx ramdisk.img signed/ramdisk.img
dtbs=`ls *.dtb`
for dtb in $dtbs; do
    ${TI_SECURE_DEV_PKG}/scripts/ift-image-sign.sh dra7xx ${dtb} signed/dtb/${dtb}
done
```

8. Create the boot FIT image using the provided ITS files (fitImage-dra7xx.its, fitImage-dra72x.its).

```
{UBOOT}/mkimage -f fitImage-dra7xx.its boot.itb
```

9. Put the device in fastboot mode and flash the images.

```
sudo fastboot oem format
sudo fastboot oem spi
sudo fastboot flash xloader u-boot-spl_HS_X-LOADER
sudo fastboot flash bootloader u-boot.img
sudo fastboot flash boot boot.itb
sudo fastboot erase environment
sudo fastboot reboot
```

Creating the system image

Signing of the Android system image is done through the Android framework infrastructure already in place. The system image verification is not enabled by default, but can be enabled by applying this patch (http://review.omapzoom.org/#/c/38243).

```
cd ${MYDROID}
cd device/ti/jacinto6evm
git fetch http://review.omapzoom.org/device/ti/jacinto6evm refs/changes/43/38243/1 && git cherry-pick FETCH_HEAD
```

The system image verification relies on the device-mapper-verity feature, so the Linux kernel must have the CONFIG_DM_VERITY option enabled.

After enabling the system partition verification, the system partition can be built using the regular Android build instructions (http://omappedia.org/wiki/6AM.1.3_Release_Notes#Building_Android_Filesystem_.28AFS.29).

6AO.1.1 Release

Verified Boot 1.0 in this release is being implemented with the TI Automotive SECDEV package for the verification of the kernel, device-tree blob and ramdisk. The Linux kernel device-mapper-verity feature is used for validation of Android system and vendor images.

Creating the boot image

The boot image is created following the same procedure documented in the previous section for Marshmallow releases. One exception is that the boot state is set to 'green' by default in HS devices. The device will not boot if the verification of x-loader, u-boot, ramdisk, kernel image or the device-tree blob failed, which corresponds to the 'red' boot state. For further information on the Verified Boot states refer to the Android documentation (https://source.android.com/security/verifiedboot/verified-boot#boot_state).

Steps

1. Apply this patch (http://review.omapzoom.org/#/c/38892/) to u-boot. For instructions about cloning the u-boot git tree, please refer to the 6AO.1.1 release notes (http://processors.wiki.ti.com/index.php/6AO.1.1_Release_Notes).

2. Follow the steps listed in the 6AM.1.2 steps (http://processors.wiki.ti.com/index.php/Android_Verified_Boot#Steps) subsection. Refer to the following sample ITS files for the different DRA7 devices supported in this release.

Creating the system and vendor images

Signing of the Android system and vendor images is done through the Android framework infrastructure already in place. Image verification is not enabled by default, but can be enabled by applying these patches (http://review.omapzoom.org/#/q/topic:avb-oreo) which set the fs_mgr's 'verify' flag to the system and vendor partitions as well as specifying the block devices for each partition.

```
cd kernel/android-4.4
git fetch http://review.omapzoom.org/kernel/omap refs/changes/09/38909/1 && git cherry-pick FETCH_HEAD
cd ${MYDROID}
```

```
cd device/ti/jacinto6evm
git fetch http://review.omapzoom.org/device/ti/jacinto6evm refs/changes/10/38910/1 && git cherry-pick FETCH_HEAD
```

The system and vendor image verification relies on the device-mapper-verity feature, so the Linux kernel must have the CONFIG_DM_VERITY option enabled.

After enabling the system partition verification, the system and vendor partitions can be built using the regular Android build instructions.

{{

1. switchcategory:MultiCore=
   - For technical support on MultiCore devices, please post your questions in the C6000 MultiCore Forum
   - For questions related to the BIOS MultiCore SDK (MCSDK), please use the BIOS Forum

   Please post only comments related to the article **Android Verified Boot** here.

Keystone=

- For technical support on MultiCore devices, please post your questions in the C6000 MultiCore Forum
- For questions related to the BIOS MultiCore SDK (MCSDK), please use the BIOS Forum

Please post only comments related to the article **Android Verified Boot** here.

C2000=*For technical support on the C2000 please post your questions on The C2000 Forum. Please post only comments about the article **Android Verified Boot** here.*

DaVinci=*For technical support on DaVincoplease post your questions on The DaVinci Forum. Please post only comments about the article **Android Verified Boot** here.*

MSP430=*For technical support on MSP430 please post your questions on The MSP430 Forum. Please post only comments about the article **Android Verified Boot** here.*

OMAP35x=*For technical support on OMAP please post your questions on The OMAP Forum. Please post only comments about the article **Android Verified Boot** here.*

OMAPL1=*For technical support on OMAP please post your questions on The OMAP Forum. Please post only comments about the article **Android Verified Boot** here.*

MAVRK=*For technical support on MAVRK please post your questions on The MAVRK Toolbox Forum. Please post only comments about the article **Android Verified Boot** here.*

*For technical s please post you questions at http://e2e.ti.cor Please post on comments abo article **Androi Verified Boot***

}}

Links

Amplifiers & Linear
Audio
Broadband RF/IF & Digital Radio
Clocks & Timers
Data Converters
DLP & MEMS
High-Reliability
Interface
Logic
Power Management
Processors

- ARM Processors
- Digital Signal Processors (DSP)
- Microcontrollers (MCU)
- OMAP Applications Processors

Switches & Multiplexers
Temperature Sensors & Control ICs
Wireless Connectivity