Secure Boot a Raspberry Pi 3 B, with u-boot and slb9670 infenion TPM2

We need a Raspberry Pi 3 B with raspbian OS, a TPM2 slb9670 Infenion and U-boot as second bootloader. U-boot on a RPi 3 B, cannot communicate with TPM slb9670, during boot. So new code added to u-boot/arch/arm/dts/bcm2837-rpi-3-b.dts. Also code added to u-boot/cmd/tpm-v2.c, so that u-boot could read non volatile memmory of slb9670 during boot.

Lets assume we have a working Raspberry Pi 3 B with Raspbian OS and a Infenion TPM slb9670 connected to SPI port. First we have to add to conig.txt three commands

dtparam=spi=on

kernel=u-boot.bin

dtoverlay=tpm-slb9670

Then we must install the TPM framework, so that the OS can communicate with TPM.

first we make an update and then install the dependecies

sudo apt-get update

sudo apt-get upgrade

sudo apt-get –y install \

autoconf-archive \

libcmocka0 \

libcmocka-dev \

procps \

iproute2 \

build-essential \

git \

pkg-config \

gcc \

libtool \

automake \

libssl-dev \

uthash-dev \

autoconf \

doxygen \

libjson-c-dev \

libini-config-dev \

libcurl4-openssl-dev \

U-boot sudo apt-get \

uuid-dev \

pandoc \

bison \

flex \

libncurses-dev

for the TPM framework

git clone <https://github.com/tpm2-software/tpm2-tss> ~/tpm2-tss

cd ~/tpm2-tss

sudo ./bootstrap

sudo ./configure

sudo make -j$(nproc)

sudo make install

sudo ldconfig

git clone <https://github.com/tpm2-software/tpm2-tss-engine> ~/tpm2-tss-engine

cd ~/tpm2-tss-engine

sudo ./bootstrap

sudo ./configure

sudo make -j$(nproc)

sudo make install

sudo ldconfig

git clone <https://github.com/tpm2-software/tpm2-tools> ~/tpm2-tools

cd ~/tpm2-tools

sudo ./bootstrap

sudo ./configure

sudo make -j$(nproc)

sudo make install

sudo ldconfig

We compile the device tree for tpm the "tpm-slb9670.dts"

dtc -@ -I dts -O dtb -o tpm-slb9670.dtbo tpm-slb9670.dts

and finaly add the compiled file "tpm-slb9670.dtbo" to boot/dtoverlay dir

We Reboot the RPi and check if TPM is working

sudo tpm2 get\_random it should return a random number from TPM

sudo tpm2 pcr\_read it should return the content of PCRs of TPM

Install the u-boot

git clone <https://github.com/u-boot/u-boot> ~/u-boot

cd ~/u-boot

replace the ~/u-boot/arch/arm/dts/bcm2837-rpi-3-b.dts, with the one provided in this repository

replace the ~/u-boot/cmd/tpm-v2.c, with the one provided in this repository

We are ready to compile u-boot

sudo make distclean

sudo make rpi\_3\_32b\_defconfig

sudo make menuconfig

Choose

Boot options

[\*] Enable preboot

(pci enum; usb start; setenv bootdelay 5) preboot default value

Library routines -> Security support

[\*] Trusted Platform Module (TPM) Support

Device Drivers -> [\*] SPI Support

[\*] Enable Driver Model for SPI drivers

[\*] Soft SPI driver

Device Drivers -> TPM support

[\*] TPMv2.x support

[\*] Enable support for TPMv2.x SPI chips

Command line interface -> Security commands

[\*] Support 'hash' command

[\*] Enable the 'tpm' command

Misc commands

[\*] gettime command

[\*] timer command

and finaly

sudo make all

the file u-boot.bin is ceated and we have to copy it to boot dir

sudo cp u-boot.bin /boot

We reboot RPi and break the booting sequence of u-boot and try some TPM commands to verify communication between u-boot and TPM.

try tpm2 init and then tpm2 info, it should return info about TPM.

Secure Boot generally means to boot the OS only if kernel files are not modified by external reasons such as virus, bad actor etc…

With a script we calculate the hash of kernel7.img and bcm2710-rpi-3-b.dtb and stores it to non volatile memory of TPM (PCR 23)

During boot the u-boot calculates the hash of kernel7.img and bcm2710-rpi-3-b.dtb and compares it with the one stored in NV memory of TPM. If they are the same then booting process is continued if not halt the booting proccess.

In a terminal, execute the script hash.sh. This script calculates the hash of kernel7.img and bcm2710-rpi-3-b.dtb and stores it to non volatile memory of TPM (PCR 23)

During boot the u-boot loads and executes the boot.scr.img which calculates the hash of kernel7.img and bcm2710-rpi-3-b.dtb and compares it with the one stored in NV memory of TPM. If they are the same then continue to boot else halt the booting.