TCB-Protection

**This document contains steps involved in enabling TCB-protection for trusted-hosts.**

# **Terminology**

**Following terminologies has been used in document:**

* **Build-host – This is the machine on which TCB-protection enabled initrd will be generated [Kernel version of build-host and trusted-hosts has to be similar]**
* **Trusted-hosts – These are the host machines, typically in data centers, which will be actually hosting measured VMs. These hosts will be booted using generated initrd by this procedure on build-host**

# **TCB-Protection Enabling for Host**

**NOTE: Please run the following scripts from current directory only where scripts exists.**

Following are the steps involved in host TCB protection enabling.

1. Generating initrd with TCB protection enabled in it
2. Creation of measurement using Trust Director (Creation of TCB-manifest.xml file)
3. Configuring trusted-hosts using TCB-protection enabled initrd

## Generating initrd with TCB protection enabled in it

### Pre-requisites

Please make sure that following pre-requisites are fulfilled before you proceed:

1. Build and copy following binaries in <TCB-ROOT>/bin directory.
   * tpmextend
   * verifier
   * rpmmio.ko

If “bin” doesn’t exist create a new directory named “bin/” in the <TCB-ROOT> directory and place the aforementioned binaries in it.

1. Kernel version of build-host should be exactly same as trusted-hosts

After fulfilling the above mentioned Pre-requisites, generate new initrd for host OS protection by following the steps:

1. Export environment variables
   * export MT\_PUBKEY="full-path-of/pubkey.pem"(Pubkey of that Mt.Wt which was used for manifest file generation)
2. Go to the <TCB-ROOT> directory and run the “generate\_initrd.sh” script.

***e.g root@ubuntu-14: cd /home/intel/TCB-Protection***

***root@ubuntu-14:/home/intel/TCB-Protection: ./generate\_initrd.sh***

This script removes any pre-existing initrd from “<TCB-ROOT>/generated\_files” directory and creates a new initrd named “initrd.img-<KERNEL-VERSION>-generic-measurement” in the “<TCB-ROOT>/generated\_files” directory.

## Creation of measurement using Trust Director (Creation of TCB-manifest.xml file)

Using Trust Director create measurement of the trusted-host and copy it as /boot/tcb-manifest.xml file on trusted-host.

<FOR STEPS REFER TRUST DIRECTOR GUIDE>

## Configuring trusted-hosts using generated TCB-protection enabled initrd

**ASSUMPTION / LIMITATION:** Root (“/”) and boot (“/boot”) of the trusted-host are on the same disk partition. (TBD: Take boot partition information as kernel argument)

Follow below mentioned steps on trusted-hosts to enable TCB-Protection:

1. Copy “initrd.img-<KERNEL-VERSION>-generic-measurement” file from <TCB-ROOT>/generated\_files folder on build-host to “/boot” of trusted-host
2. Copy “tcb-manifest.xml” file from Trust Directory host to “/boot” of trusted host
3. Configure grub entry on trusted host.
   1. Create a duplicate grub menuentry of the current tboot grub menuentry in the /etc/grub/grub.cfg [Note: It’s better to keep original entry unmodified so that incase of unwanted condition, host could be booted with original initrd and error can be fixed]
   2. Modify copied grub menuentry to add
      1. Modify name of the menuentry
      2. Initrd module – Name of the copied initrd file “initrd.img-<KERNEL-VERSION>-generic-measurement”
      3. Additional kernel argument “tpm\_major\_version” – TPM version of the trusted-host. Version 1 uses SHA1 hash of measurement to update TPM’s PCR-19. Other versions uses SHA256 hash of measurement.

Here is the sample menuentry. Modified values are highlighted in RED.

Menuentry ‘***TCB-Protection* Ubuntu – tboot**’ --class ubuntu --class gnu-linux --class gnu --class os --class tboot {

insmod part\_msdos

insmod ext2

set root='hd0,msdos1'

if [ x$feature\_platform\_search\_hint = xy ]; then

search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1 --hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1 e9b96055-6bbf-45fb-9040-e7f28d84e91b

else

search --no-floppy --fs-uuid --set=root e9b96055-6bbf-45fb-9040-e7f28d84e91b

fi

echo 'Loading tboot 1.8.1 ...'

multiboot /boot/tboot.gz /boot/tboot.gz logging=serial,vga,memory

echo 'Loading Linux 3.13.0-32-generic ...'

module /boot/vmlinuz-3.13.0-32-generic /boot/vmlinuz-3.13.0-32-generic root=UUID=e9b96055-6bbf-45fb-9040-e7f28d84e91b ro biosdevname=0 intel\_iommu=on ***tpm\_major\_version=1***

echo 'Loading initial ramdisk ...'

***module /boot/initrd.img-3.13.0-32-generic-measurement /boot/initrd.img-3.13.0-32-generic-measurement***

echo 'Loading sinit 3rd\_gen\_i5\_i7\_SINIT\_67.BIN ...'

module /boot/3rd\_gen\_i5\_i7\_SINIT\_67.BIN /boot/3rd\_gen\_i5\_i7\_SINIT\_67.BIN

}

Now reboot the system using the grub entry just created.