TCB-Protection

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

# **Terminology**

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

* **Build-host – This is the host machine on which TCB-protection related artifacts will be generated**
* **Trusted-hosts – These are the host machines, typically in data centers, which will be actually hosting measured VMs. These hosts will be booted using artifacts generated by this procedure on build-host**

# **TCB-Protection Enabling**

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

TCB protection enabling is 2 phase process.

Phase – 1 is generation TCB protection enabled artifacts on build-host

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

Phase – 2 is using generated artifacts boot Trusted hosts in data center

1. Booting trusted-hosts using generated root file system and initrd to enable

## Phase – 1: Generate TCB protection enabled artifacts

### Pre-requisites:

Make sure that a build-host machine is configured with all required packages and components on it. This must include following but not limited to these

* vRTM
* Policy Agent (Mystery Hill Agent)
* Trust Agent
* Tboot, trousers, etc. packages

Basically, this host machine should have all required installations done as the same would be replicated across all the trusted-hosts in data center which will be TCB-protection enabled using artifacts generated by this process. There should be no need to install any additional software on trusted-hosts.

### Creation of root file system

Once build-host is configured completely, first step is to create a tarball of root file system of build-host. For this following script needs to be executed.

**./create\_rootfs\_tarball.sh**

It will take necessary inputs from user on console.

After successful execute of this script a “rootfs.tar.gz” will get generated in "./kvm\_pre\_generated\_files” or “xen\_pre\_generated\_files" depending on the option user had selected.

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

Once rootfs.tar.gz is generated, next step is to take measurement of required files and folders inside it using Trust Director. Output of this step would be a manifest.xml file.

* Generate manifest XML for the generate rootfs.tar.gz using Trust Director (TD would be installed on some different machine. So, user needs to copy rootfs.tar.gz to appropriate location and then generate manifest.xml)
* Copy the generate manifest.xml file in the same folder where rootfs.tar.gz was generated
* Rename “manifest.xml” file to "tcb­manifest.xml"

### Generating initrd with TCB protection enabled in it

Next step is to generate initrd which contains required binaries and scripts so that on booting trusted-hosts first measurement of rootfs.tar.gz happens and then host starts up.

Generate new initrd for host OS protection by following the steps:

* Export environment variables
  + export RPROOT="full/path/to/rpcore/in/git/repository" (e.g. /home/intel/git-repositories/mysteryhill/rpcore)
  + export MT\_PUBKEY="full-path-of/pubkey.pem"(Pubkey of that Mt.Wt which was used for manifest file generation)
* Run the script

**./generate\_initrd.sh**

This script will generate "initrd\_-<KERNEL-VERSION>-generic " file in the same folder ("./kvm\_pre\_generated\_files” or “./xen\_pre\_generated\_files"). This will also copies kernel of the same machine to this folder “vmlinuz-<KERNEL\_VERSION>-generic”.

**NOTE: For now this script builds imvm (verifier), rpmmio and tpmextend and copies binaries in initrd. So, machine on which initrd is getting generated requires necessary packages like make, gcc, etc. to build these sources. Later, we can modify this to build and copy binaries from some other machine to this machine so that need not other pre-requisites. In that case, machine on which rpmmio is getting build must have same kernel-version as of initrd & rootfs.tar.gz to work properly.**

At this point, all required artifacts are generated for enabling any host with TCB-protection. All this artifacts should be in either "./kvm\_pre\_generated\_files” or “./xen\_pre\_generated\_files" folder. Following is the list of files expected in this folder:

1. rootfs.tar.gz
2. tcb-manifest.xml
3. initrd\_<KERNEL\_VERSION>-generic
4. vmlinuz-<KERNEL\_VERSION>-generic

Now, you need to download SINIT script from https://software.intel.com/en-us/articles/intel-trusted-execution-technology and copied in the appropriate folder ("./kvm\_pre\_generated\_files” or “./xen\_pre\_generated\_files").

1. 3rd\_gen\_i5\_i7\_SINIT\_67.BIN (Just an example)

Note: Download the SINIT.bin file according to the processor of the trusted-hosts. Also, make a note that this needs to be .bin file and not .zip.

## Phase – 2 Trusted booting hosts

<TBD: How to boot trusted host first time?>

For now let’s assume that you have some OS installed on the host which you want to make trusted-host.

Copy "./kvm\_pre\_generated\_files” or “./xen\_pre\_generated\_files" folder from build-host to trusted-host.

Copy following scripts from build-host to trusted-host and put it at same level as "./kvm\_pre\_generated\_files” or “./xen\_pre\_generated\_files" so that it looks like below:

* <TCB-Protection DIR>
  + kvm\_pre\_generated\_files/ OR xen\_pre\_generated\_files/
  + tcb-main-script.sh
  + setup\_encrypted\_lvm.sh
  + configure\_trusted\_host.sh

### Booting trusted-hosts using generated root file system and initrd to enable

Go to <TCB-Protection DIR> directory and run following script:

**./tcb-main-script.sh**

This will ask inputs from user on console. It will provide option to create LVM to use it as storage (where disks for measured VMs will be hosted). It will also configure host to be booted as trusted host.

TBD: How TA will take ownership of the TPM of the trusted-host? Also, configuration files related to TA needs to be persisted on storage for reboot scenario.