**Steps for TCB-Protection**

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

**Assumption:**

* Host OS with all required packages and components is prepared
* Create\_rootfs\_tarball.sh script will include almost all the files of the Host OS in root FS tarball. You can add / remove folders by editing script, if necessary.

1. Create rootfs tarball using a script [Execute this script on preinstalled Host OS to generate root FS which will be used on all Hosts booted using this TCB]

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

The file gets created in "./kvm or xen\_pre\_generated\_files"

2. Generate Manifest xml with this rootfs tarball using Trust Director.

3. Rename the generated manifest file to *"tcb-manifest.xml"* and place it in that pre\_generated\_files folder for the respective hypervisor.

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

(4.1) Export envirnoment variable

export RPROOT="full/path/to/rpcore/in/git/repository" (e.g. /home/intel/git-repositories/mysteryhill/rpcore)

(4.2) export MT\_PUBKEY="full-path-of/pubkey.pem"(Pubkey of that Mt.Wt which was used for manifest file generation).

(4.3)Run the script

***./generate\_initrd.sh***

The file "inirtd.img-kernel-version "gets generated in   
"./kvm or xen\_pre\_generated\_files"

5. Check if the following files exist in the folder  
"./kvm or xen\_pre\_generated\_files"

*5*.1 rootfs.tar.gz

5.2 tcb-manifest.xml

5.3 initrd\_KERNEL\_VERSION-generic

**5.4 3rd\_gen\_i5\_i7\_SINIT\_67.BIN**

This files needs to be downloaded from the following location

<https://software.intel.com/en-us/articles/intel-trusted-execution-technology> and copied in the kvm or xen pre\_generated\_files directory.

5.5 vmlinuz-KERNEL\_VERSION-generic

Following steps needs to do on the host where TCB protections needs to enabled:

1. Run the script

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

This script will set up LVM and will configuring Trusted Host.

This is a wrapper script for following 2 scripts

***./setup\_encrypted\_lvm.sh*** & ***./configure\_trusted\_host.sh***