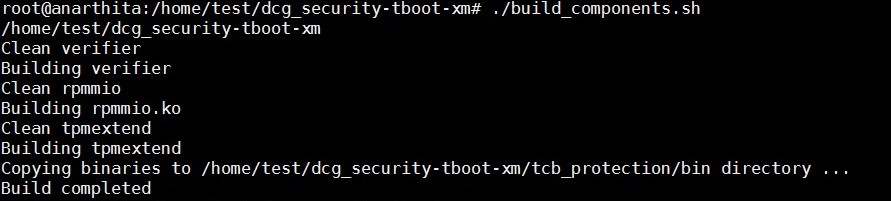
Building Measurement Agent for TCB - v3

Assumption: For the ease of testing the first build of TCB protection, below steps are assuming that the build would be built on the same host where it would be installed. Need to tweak few steps where we would build the image on build server and would be deployed on a different server.

Note: Steps mentioned below are same for Ubuntu, RHEL & Fedora unless mentioned explicitly.

* Check out the latest code from dev 1.x branch
  + This code is currently copied to [\\fmcsssan101\CSSShare\Projects\MysteryHill\Measurement Agent\Build](file:///\\fmcsssan101\CSSShare\Projects\MysteryHill\Measurement%20Agent\Build) 1
  + Copy this code on the host where we need to enable TCB protection (Ex: /root/MeasurementAgent)
* Modify the permissions for build\_components.sh if needed (766)
* Run the build\_components.sh with --installpkg option. This will ensure that all the required packages are installed.
  + If in the package installation fails ensure that proper http proxy settings are exported. Logout and log back in.
  + For Fedora / RHEL: Make sure that required packages are available in Intel’s internal repository. If not either add packages to repository or download and install from some external repository

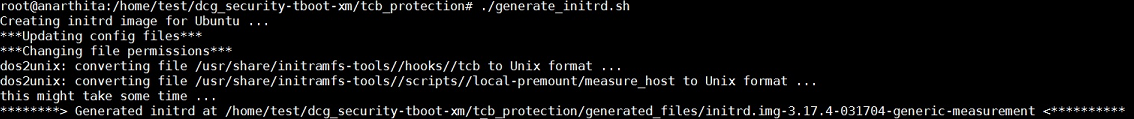


* After the build is successful, the built components are available under the /tcb\_protection/bin folder as shown below.

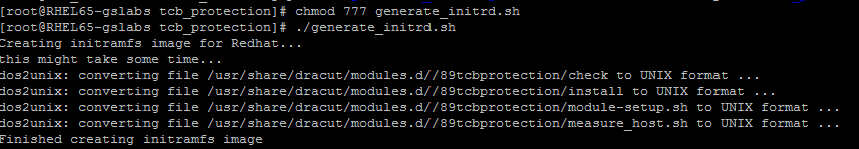
Machine generated alternative text:
total 32
drwxr—xr—x 6 root root 4096 Mar 10 03:04 .!
drwx 12 root root 4096 Mar 10 03:28 ..,
—rwxrw—rw— 1 root root 2467 Mar 10 03:12 build components.sh*
drwxr-xr-x 4 root root 4096 Mar 10 03:11 imvni/
—rw—r——r—— 1 root root 3378 Mar 10 03:11 outfile
drwxr—xr—x 3 root root 4096 Mar 10 02:59 rpnmio/
drwxr-xr-x 6 root root 4096 Mar lO 03:08 tcbprctection/
drwxr-xr-x 4 root root 4096 Mar 10 03:04 tpmextend/
root@ubuntul2o4 : -fverifier# cd tcb_protectionfbin
root@ubuntul2o4 : —fverifier/tcbprotection/bin# 11
total 92
drwxr—xr—x 2 root root 4096 Mar 10 03:04 .!
drwxr—xr—x 6 root root 4096 Mar 10 03:08 ..!
—rwxr—xr—x 1 root root 17281 Mar 10 03:11 rpmmio.lco*
—rwxr—xr—x 1 root root 16762 Mar 10 03:11 tpmextend*
—rwxr—xr—x 1 root root 43232 Mar 10 03:11 verifier*
root€ubuntul2o4 : —fverifier/tcb protection/binS •

* Go to the /tcb\_protection folder. Update the permissions if needed for both the scripts.
* Run the "generate\_initrd.sh" script.
* Sample output of the .generate\_initrd.sh script

For Ubuntu:



For RHEL (for Fedora it would be almost similar to this):



* "generate\_initrd.sh" script would create the new initrd image under the "generated\_files" folder.

Machine generated alternative text:
root@MW-l404—SB: -/verifier/tcbprotection$ 11
total 44
drwxr—xr-x 6 root root 4096 Mar 12 02:02 .!
drwxr-xr-x 6 root root 4096 Mar 12 01:56 ..,
drwxr—xr-x 2 root root 4096 Mar 12 01:56 bin!
-rwxrw-rw— 1 root root 4281 Mar 11 10:21 configure hostsh*
—rw—r——r—— 1 root root 1084 Mar 11 10:21 create_menuentry.pl
drwxr—xr-x 2 root root 4096 Mar 12 01:58 generated files!
—rwxrw—rw— 1 root root 3593 Mar 10 02:20 generate_initrd.sh*
drwxr—xr-x 2 root root 4096 Mar 12 01:51 initrdhooicsf
drwxr—xr-x 2 root root 4096 Mar 12 01:51 local—premountf
—rw—r——r-- 1 root root 1018 Mar 12 02:02 saraplemenuentry
root@MH—1404—SB: -íverifier!tcb_protection* 11 generated_files!
total 22336
drwxr-xr-x 2 root root 4096 Mar 12 01:58 .!
drwxr—xr-x 6 root root 4096 Mar 12 02:02 ..!
—rw—r——r-— 1 root root 22859825 Mar 12 01:58 initrdimg—313.0—24—generic—measurenent
root@MH—1404—SB: -íverifier!tcb_protection# • ___________ _____________

* You can verify if the image was created successfully and having all the Measurement Agent components by running the following command
  + lsinitramfs initrd.img-3.2.0-65-generic-measurement | grep "rpmmio.ko"
* Ensure that the manifest file exists before executing the next step. A sample is show below. It can be modified to add any File or Directory.

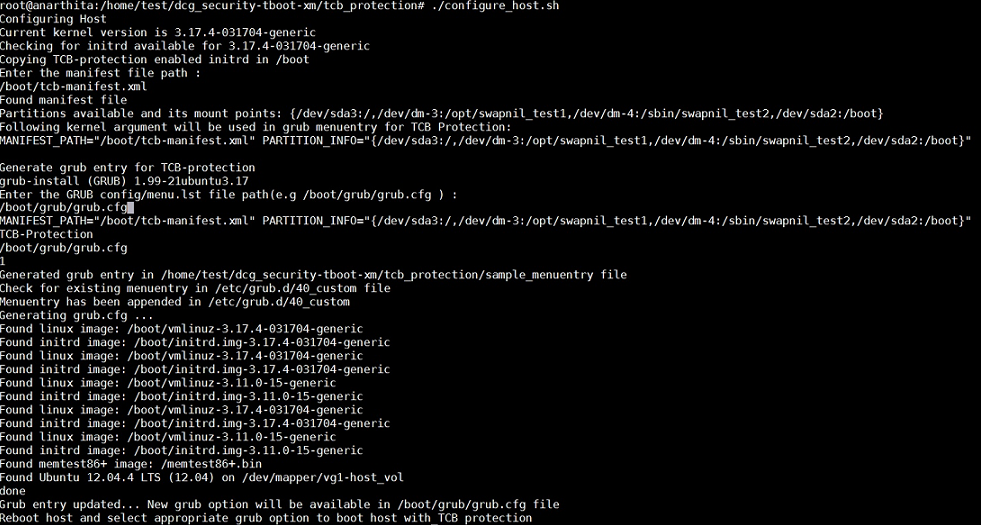
<?xml version="1.0"?>

<Manifest digestAlg="sha1">

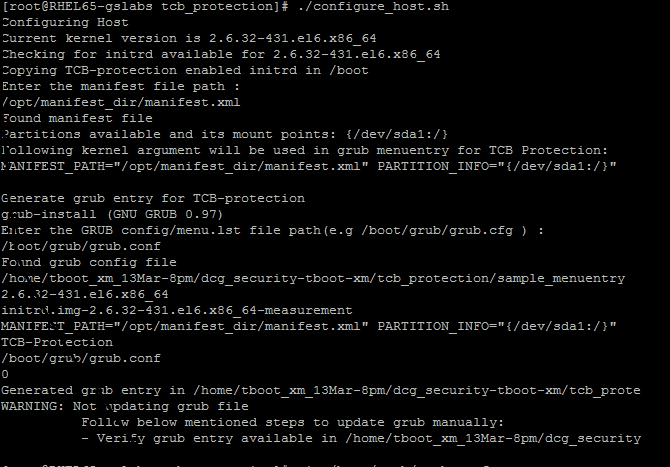
<File Path="/root/trustagent.env"/>

</Manifest>

* Run the "configure\_host.sh" script. As shown in the output below, the script would get the manifest file and grug.cfg file path as input from the user, and creates grub entry in ./sample\_menuentry file. It behaves differently based on Grub version used. By default, Ubuntu 12.04+ & Fedora 20+, RHEL 7+ uses grub 2. RHEL 6.x uses grub legacy.
* For Ubuntu / Fedora [OS with Grub 2]: This script will also append generated grub entry in /etc/grub/40\_custom file and do update-grub to update grub.cfg automatically. Following is the output for Ubuntu [Similar output will get generated for Fedora as well]
  + Note: Incase if grub entry for TCB-Protection is already available in 40\_custom config then this script will not update it automatically and will give WARNING message with instructions. In this case, grub entry would be available in ./sample\_menuentry file which needs to verified and copied OR replaced in 40\_custom file and then run command to update grub.cfg as mentioned in instructions on console



* For RHEL (with Grub legacy), this script will populate grub entry in ./sample\_menuentry file which needs to be verified and copied to grub.cfg / menu.lst file



Grub entry for Ubuntu / Fedora (Grub 2) will look like below:

Machine generated alternative text:
menuentry ‘TOE-Protection Ubuntu GNU/Linux, with tboot 1.8.1 and Linux 3.13.0—24-generic’ ——class ubuntu ——class gnu—linux ——class gnu ——class os ——class tboot {
savedefault
insmod part_msdos
insmod ext2
set root=
if [ x$featureplatform_searchjiint = xy J
search --no-floppy --fs-uuid --set= ---hint-bios=hd0,rrtsdosl ——hint—efihdo,rnsdosl ——hint—baremetalahci0,msdcsl c8Sael6a—046f—4784—8c92—6fbcdcaf4lso
else
search ——no—floppy ——fs—uuid ——set= - : r LE: - 46f—4784—8c92—6fbcdcaf4l5o
fi
echo ‘Loading tboot 1.8.1 ...‘
multiboot /tboot.gz /tboot.gz loggin
echo ‘Loading Linux 3.13.0—24—generic ...‘
module /vmlinuz—3.13.0—24—generic /vmlinuz—3.13.0—24—generic root= :r:, ___-r_:::: r: izrrl: on ZFESJEAJE-=” r::: ::rnifest.zanl” PARTITION_1NY0”{/dev/znapper/NIi——14
echo ‘Loading initial ramdisk . ..‘
module /initrd.img—3.13.0—24—generic—measurement /initrd.img—3.13.0—24—generic—measurement
I

Grub entry for RHEL (grub legacy) looks like below:

