TCB-Protection on Windows

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 tbootxm driver 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 generated tbootxm driver installed on them

## How TCB-Protection works for Host

TCB-Protection for host is used to make sure that root file system of the trusted host is not modified while system boots up. To achieve this host should have TPM capability.

1. List of files are added in manifest for host measurement and extending PCR values
2. Verifier code, ported to driver, gets called during system boot and it measures all files mentioned in manifest.xml file (location of manifest.xml file on host has been hard coded inside driver)
3. Result of the verification is used to extend PCR-14 value so that later Trust Agent and Mt Wilson can use this value to attest host

# TCB-Protection Enabling for Host

Following are the steps involved in host TCB protection enabling.

1. Installing tbootxm driver
2. Creation of measurement using Trust Director (Creation of manifest.xml file)
3. Configuring trusted-hosts using installed tbootxm driver

## Installing tbootxm driver

### Pre-requisites

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

1. Build the tbootxm driver using required configuration (OS type).
2. Run the nsis script to generate its installer.

**Installation**

1. Copy the installer from build-host to trusted-host.
2. Run the tbootxm installer which will install the driver.

## 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 C:/manifest.xml file on trusted-host.

<FOR STEPS REFER TRUST DIRECTOR GUIDE>

## Configuring trusted-hosts using installed tbootxm driver

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

1. Make sure that “C:\Windows\Logs\MeasuredBoot” directory exists. If not then create it. This is the directory where measurement.xml file gets generated.
2. Copy “manifest.xml” file from Trust Director ssto “C:” directory of trusted host.
3. Now reboot the system.