TRUSTED EXECUTION TECHNOLOGY AND TBOOT IMPLEMENTATION

2009-2010 p/w Mobile Platforms (Montevina/Calpella)

Table of Contents:

Introduction

HP has implemented the Trusted eXecution Technology (TXT), part of Intel's Safer Computing Initiative, on certain models of 2009-2010 commercial notebooks. The purpose of this document is to provide a step by step guideline to setup a TXT enabled environment.
The document will cover the following areas:

- BIOS settings related to TXT,
- Intel's Trusted Execution Technology,
- Trusted Boot and
- Launch Control Policies

Trusted eXecution Technology (http://www.intel.com/technology/security/), a hardware-based mechanism that helps to protect against software-based attacks and protects the confidentiality and integrity of data stored or created on the client PC by means of measured launch and protected execution. In other words, TXT provides only the launch-time protection, i.e. ensure that the code we load, is really what we intended to load - secure and not compromised by any virus attacks. (http://download.intel.com/technology/security/downloads/315168.pdf).

The technology mainly depends on set of hardware extensions to Intel processors and chipsets that boost the platform with security capabilities. Trusted Platform Module is another important hardware component. The TPM module is used to store and compare hash values (of launched environment), which provides much greater security than storing them in software or on the hard disk

Trusted boot (Tboot), an open source, pre- kernel/VMM module that uses Intel(R) Trusted Execution Technology (Intel(R) TXT) to perform a measured and verified launch of an OS kernel/VMM (http://sourceforge.net/projects/tboot, http://www.bughost.org/repos.hg/tboot.hg).

Launch Control Policy (LCP) is a verification mechanism used to verify the Intel TXT 'verified launch' processes. Based on the criteria/choice defined in the Platform Default (PD) policy set by the Platform Supplier (PS) or the Platform Owner (PO) policy set by the owner, the LCP determines whether the current platform configuration or environment meets the requirements and can be launched.

System Requirements

- Trusted Platform Module (TPM 1.2), TXT and Virtualization Technology (VT) supported chipset (vPro platforms).
- TPM – Locked, Enabled and Activated, VT- Enabled, TXT- Enabled (discussed in next section)

BIOS TXT Settings

Enter BIOS Setup by pressing F10 during POST and execute the following steps:

1. Go to **Security → Setup BIOS Administrator Password** to enter the BIOS administrator password.
2. Go to **Security → TPM Embedded Security → Embedded Security Device State → Enabled**
3. Go to **System Configuration → Device Configurations → Virtualization Technology → Enabled**
4. Go to **System Configuration → Device Configurations → SATA Native Mode → IDE** (optional)

   Note: If you expect to use RAID option at some point in the future, then it is advisable to use AHCI/RAID option instead of IDE. Switching from IDE to AHCI/RAID will result in "Kernel Panic" message and makes it impossible to boot to Fedora unless you switch the SATA option back to IDE
5. Save settings and exit F10 and reboot.

Enter BIOS setup by pressing F10 during POST, execute the following steps:

1. Go to System **Configuration → Device Configurations → TXT Technology → Enabled**
2. Save settings and exit F10 and reboot.

Fedora Installation

1. Download the image of Fedora 7/8 (64bit) and burn it on DVD.
2. Start the Fedora installation. If you see any "Kernel Panic –" message or if the installation hangs, try adding "acpi=off" as kernel arguments (hit tab) at the grubloader.
3. At the "Disk Partitioning Setup" screen, select from the Drop down Menu, <Create custom Layout>, press <Next>
4. Delete any existing partitions.
5. Next add 3 partitions as follows and Press <Next>:

   1st: mount Point: "/boot", file type = ext3, size = 400

   2nd: file type: swap, size = 2048

   3rd: mount point = "/", file type = ext3, size = fill to max

6. Don't install boot loader password or select 'configure advance boot loader options'. Press <Next>

7. At the next screen, select the time zone and after that choose a password of your choice (the default username is 'root').
8. Install All Software packages, 1) office and productivity, 2) Software development, 3) Web Server. Don't install 'Additional Fedora Software'. Press <Next>
9. After installation is complete the system will ask for a reboot for the changes to take effect.
10. After the first reboot select the following settings: "Firewall" - Disabled, "Security Enhanced Linux <SELinux>" - Disabled. The system will prompt for a restart after the settings are made.

Note: When you boot into Fedora, at the login screen, if you get an error stating that X server has failed to start, try to configure the x server and set the color depth to "Thousands of colors" instead of "Millions of colors". For any other situation where the display is not visible (black screen) you may have to edit xorg.conf file and make the "Default Depth" to 16 under "Screen" section

XEN 3.4.3 Installation

1. Boot to Fedora. Install the Ethernet drivers if you haven't already done (latest drivers are available at http://sourceforge.net/projects/e1000/files/e1000e%20stable/).
2. Open terminal,
3. If required set the proxy options as, export http_proxy=<proxy address>:<port number>
4. yum install mercurial (Installs latest version of mercurial from internet if you haven't already installed it).
5. Install wget if not already installed and download Xen 3.4.3 version into the root directory,
   a. yum install wget
   b. wget **http://bits.xensource.com/oss-xen/release/3.4.3/xen-3.4.3.tar.gz**
   c. wget **http://bits.xensource.com/oss-xen/release/3.4.0/linux-2.6.18-xen-3.4.0.tar.gz** download this in the same root location.
6. Check if the following packages are installed ('yum list <packageaname>' will display 'installed', else it would say 'fedora'). If not then install using 'yum install <packagename>'. :yum list gcc make binutils zlib python ncurses openssl bridge-utils iproute udev dev86 unifdef imake isdn4k-utils iasl.
7. tar –xzvf linux-2.6.18-xen-3.4.0.tar.gz
8. cd linux-2.6.18-xen-3.4.0
9. make mrproper
10. make menuconfig
11. In the Linux Kernel Configuration window set/select the following options
    d. General Setup → Local Version - "-xen" (without the quotes)
    e. Processor type and features → Enable Xen compatible kernel - * (implies built-in)
    f. Device Drivers → SCSI device support →SCSI low-level drivers – Select 'M' on all excluded options (M, implies Module)
    g. XEN → Privileged Guest (domain 0) - *
    h. XEN → - unselect/exclude all "frontend driver"
12. After setting these options keep pressing ESC until prompted to save the kernel configuration. Choose Yes to save settings.
13. make (this takes >30 minutes)
14. make modules_install
15. make install
16. cd ..

17. tar -xzvf xen-3.4.3.tar.gz
18. cd xen-3.4.3
19. make install-xen
20. make install-tools
21. edit the menu file (/boot/grub/menu.lst) and add the following grub entry:

    title Fedora Xen 3.4.3 (2.6.18.8-xen)

    root (hd0,0)

    kernel /xen-3.4.3.gz iommu=required

    module /vmlinuz-2.6.18.8-xen ro root=LABEL=/ rhgb

    module /initrd-2.6.18.8-xen.img

22. Make sure to check the root location and 'root=LABEL=/' match with the first grub entry and points to the root partition.
23. Reboot the system. Enable TPM, VTD and TXT in the BIOS if not already done.
24. The next time you boot into the system, you can select the option at the boot menu to boot into 'Fedora Xen 3.4.3 (2.6.18.8-xen)'.

TBOOT Installation

1. Depending upon the platform copy the appropriate latest sinit.bin file into /boot directory. The file can be located at http://sourceforge.net/projects/tboot/files/
2. Open the terminal
3. cd ~/
4. If required set the proxy options as, export http_proxy=<proxy address>:<port number>
5. yum install mercurial (if not installed already)
6. wget http://downloads.sourceforge.net/project/trousers/trousers/0.3.5/trousers-0.3.5.tar.gz
7. tar -xzvf trousers-0.3.5.tar.gz
8. cd trousers-0.3.5
9. sh bootstrap.sh
10. ./configure
11. make
12. make install
13. hg clone –r 9c733d6c3f40 **http://www.bughost.org/repos.hg/tboot.hg** (this downloads tboot package of the revision mentioned)
14. cd tboot.hg/tboot
15. edit Config.mk, un-comment (remove #) the line #CFLAGS += -DMEM_LOGGING and save it (This will write all of the serial messages to a memory buffer. Helpful for notebooks that lack serial output port).
16. cd ..
17. make install
18. edit the menu.lst to additional grub entry:

    title Fedora Tboot (2.6.18.8-xen)

    root (hd0,0)

kernel /tboot.gz logging=serial,vga,memory

module /xen-3.4.3.gz iommu=required

module /vmlinuz-2.6.18.8-xen ro root=LABEL=/ rhgb

module /initrd-2.6.18.8-xen.img

module /sinit.bin

19. Make sure to check the root location and 'root=LABEL=/' match with the first grub entry and points to the root partition.
20. Reboot the system. Enable TPM, VTD and TXT in the BIOS if not already done.
21. The next time you boot into the system, you can select the option at the boot menu to boot into 'Fedora Tboot (2.6.18.8-xen)'.

Note: If the unit hangs after you boot into Tboot at the boot menu, check if you have any USB devices plugged in to your unit. Also disable USB Legacy Support in your BIOS settings (under F10: System Configuration → Device Configurations → USB legacy Support) and try to boot into Tboot again.

TPM TOOLS 1.3.5 Installation

1. Open the terminal
2. cd ~/
3. If required set the proxy options as, export http_proxy=<proxy address>:<port number>
4. Install wget if not already installed (yum install wget)
5. wget http://internap.dl.sourceforge.net/sourceforge/trousers/tpm-tools-1.3.5.tar.gz
6. Make sure you have 'automake', 'autoconf', 'libtool', 'gettext', 'gettext-devel' and 'trousers' installed.
7. tar –xzvf tpm-tools-1.3.5.tar.gz
8. cd tpm-tools-1.3.5
9. sh bootstrap.sh
10. ./configure
11. make
12. make install

LCP: Define Platform Owner Policy

Take TPM Ownership:

1. Open the terminal
2. sudo –s
3. ldconfig /usr/local/lib (in case of FC8 you may have to try '/sbin/ldconfig /usr/local/lib')
4. modprobe tpm_tis (in case of FC8 you may have to try '/sbin/modprobe tpm_tis')
5. tcsd (in case of FC8 you may have to try '/usr/sbin/tcsd')
6. tpm_takeownerhip –z (create owner password. In case of FC8 you may have to try '/usr/local/sbin/tpm_takeownerhip –z')

Define TPM NV indices for polices:

7. **For 2009 Montevina Platforms only:**

   tpmnv_defindex -i owner -p <ownerauth password> (creates owner index)

For 2010 Calpella Platforms only:

tpmnv_defindex -i owner -s 0x36 -p <ownerauth password> (creates owner index)

8. tpmnv_defindex -i 0x20000001 -s 512 -pv 0x02 -p <ownerauth password> (creates index 0x20000001 for verified launch policies. This index is hardcoded in tboot source code, so you can't use any other index to write the verified launch policies. If this command gives errors related to available space in TPM NV, try 256 instead of 512)

Create and Write LCP policies to TPM NV (implemented by SINIT):

9. mkdir –p /tmp/temp
10. cd /tmp/temp
11. lcp_mlehash –c "logging=serial,vga,memory" /boot/tboot.gz > tboot_hash
12. **For 2009 Montevina Platforms only:**

    lcp_crtpol -t hashonly -m tboot_hash –o lcp.pol

    lcp_writepol -i owner -f lcp.pol -p <ownerauth password>

    For 2010 Calpella Platforms only:

    lcp_crtpolelt --create --type mle --ctrl 0x00 --out mle.elt tboot_hash

    lcp_crtpollist --create --out list_unsig.lst mle.elt

    lcp_crtpol2 --create --type list --pol owner_list.pol --data owner_list.data list_unsig.lst

    cp owner_list.data /boot

    lcp_writepol -i owner -f owner_list.pol -p <ownerauth password>

Create and Write Verified Launch policies to TPM NV (implemented by Tboot):

13. tb_polgen –create –type nonfatal tcb.pol
14. tb_polgen –add –num 0 –pcr 18 –hash image –cmdline "iommu=required" –image /boot/xen.gz tcb.pol (all in a single line. Make sure that the command line parameters via –cmdline, MUST match the parameters as specified in /boot/grub/menu.lst EXCLUDING the name of the file)
15. tb_polgen –add –num 1 –pcr 19 –hash image –cmdline "ro root=LABEL=/ rhgb" –image /boot/vmlinuz-2.6.18.8-xen tcb.pol (all in a single line)
16. tb_polgen –add –num 2 –pcr 19 –hash image –cmdline "" –image /boot/initrd-2.6.18.8-xen.img tcb.pol(all in a single line)
17. lcp_writepol -i 0x20000001 -f tcb.pol -p <ownerauth password>

Note: Please refer to the "Intel Trusted Execution Technology- Launch Control Policy: Linux Tools User Manual" for the proper usage of other related commands

Appendix A

Sample Tboot serial output captured on 2010 Calpella platform(The actual output may vary depending on the system configuration):

Intel(r) TXT Configuration Registers:
STS: 0x000188c1
senter_done: TRUE
sexit_done: FALSE
mem_unlock: FALSE
mem_config_lock: TRUE
private_open: TRUE
mem_config_ok: TRUE
ESTS: 0x00
txt_reset: FALSE
txt_wake_error: FALSE
E2STS: 0x0000000000000006
slp_entry_error: FALSE
secrets: TRUE
block_mem: TRUE
reset: FALSE
ERRORCODE: 0x00000000
DIDVID: 0x0000000fa0008086
vendor_id: 0x8086
device_id: 0xa000
revision_id: 0xf
SINIT.BASE: 0x77700000
SINIT.SIZE: 131072B (0x20000)
HEAP.BASE: 0x77720000
HEAP.SIZE: 917504B (0xe0000)
DPR: 0x0000000077800041
lock: TRUE
top: 0x77800000
size: 4MB (4194304B)
****
TXT measured launch: TRUE
secrets flag set: TRUE
****
ERROR: cannot map heap
TBOOT log:
max_size=7fe4
curr_pos=4ecb
buf:
T: ********** TBOOT **********

TBOOT: unavailable
TBOOT: **
TBOOT: command line: logging=serial,vga,memory
TBOOT: TPM is ready
TBOOT: TPM nv_locked: TRUE
TBOOT: read verified launch policy (**512 bytes**) from TPM NV
TBOOT: policy:
TBOOT: version: 2
TBOOT: **policy_type**: TB_POLTYPE_CONT_NON_FATAL
TBOOT: hash_alg: TB_HALG_SHA1
TBOOT: policy_control: 00000001 (EXTEND_PCR17)
TBOOT: **num_entries**: 3
TBOOT: policy entry[0]:
TBOOT: mod_num: 0
TBOOT: pcr: 18
TBOOT: hash_type: TB_HTYPE_IMAGE
TBOOT: num_hashes: 1
TBOOT: **hashes[0]**: 75 e6 10 32 35 f4 72 3d 93 ff ed fd 3b df b6 6c 02 e2 3c 12
TBOOT: policy entry[1]:
TBOOT: mod_num: 1
TBOOT: pcr: 19
TBOOT: hash_type: TB_HTYPE_IMAGE
TBOOT: num_hashes: 1
TBOOT: **hashes[0]**: 90 c6 1f 2d 92 89 a9 ad 57 cc 36 57 79 c8 74 fb ba a1 d0 ae
TBOOT: policy entry[2]:
TBOOT: mod_num: 2
TBOOT: pcr: 19
TBOOT: hash_type: TB_HTYPE_IMAGE
TBOOT: num_hashes: 1
TBOOT: **hashes[0]**: 80 14 c6 56 fb 3d 33 ed 97 bd 08 d2 8f 35 f5 54 21 6c d4 3c
TBOOT: TPM: write nv 20000002, offset 00000000, 00000004 bytes, return = 00000002
TBOOT: Error: write TPM error: 0x2.
TBOOT: IA32_FEATURE_CONTROL_MSR: 0000ff07
TBOOT: CPU is SMX-capable
TBOOT: CPU is VMX-capable
TBOOT: SMX is enabled
TBOOT: TXT chipset and all needed capabilities present
TBOOT: TPM: write nv 20000002, offset 00000000, 00000004 bytes, return = 00000002
TBOOT: Error: write TPM error: 0x2.
TBOOT: LT.ERRORCODE=0
TBOOT: LT.ESTS=0
TBOOT: IA32_FEATURE_CONTROL_MSR: 0000ff07
TBOOT: CPU is SMX-capable

TBOOT: CPU is VMX-capable
TBOOT: SMX is enabled
TBOOT: TXT chipset and all needed capabilities present
TBOOT: bios_data (@77720008, 2c):
TBOOT: version: 3
TBOOT: bios_sinit_size: 0x0 (0)
TBOOT: lcp_pd_base: 0x0
TBOOT: lcp_pd_size: 0x0 (0)
TBOOT: num_logical_procs: 4
TBOOT: flags: 0x00000000
TBOOT: TPM: write nv 20000002, offset 00000000, 00000004 bytes, return = 00000002
TBOOT: Error: write TPM error: 0x2.
TBOOT: CR0 and EFLAGS OK
TBOOT: no machine check errors
TBOOT: CPU is ready for SENTER
TBOOT: checking previous errors on the last boot.
TPM: read nv index 20000002 offset 00000000, return value = 00000002
TBOOT: Error: read TPM error: 0x2.
TBOOT: last boot has no error.
TBOOT: checking whether module 4 is an SINIT AC module...
TBOOT: ACM size is too small: acmod_size=50, sizeof(acm_hdr)=4
TBOOT: : failed.
TBOOT: checking whether module 3 is an SINIT AC module...
TBOOT: : succeeded.
TBOOT: **user-provided SINIT found: /sinit.bin**
TBOOT: chipset ids: vendor=8086, device=a000, revision=f
TBOOT: 1 ACM chipset id entries:
TBOOT: vendor=8086, device=a000, flags=1, revision=1, extended=0
TBOOT: copied SINIT (size=85c0) to 77700000
TBOOT: **AC mod base alignment OK**
TBOOT: AC mod size OK
TBOOT: AC module header dump for SINIT:
TBOOT: type: 0x2 (ACM_TYPE_CHIPSET)
TBOOT: length: 0xa1 (161)
TBOOT: version: 0
TBOOT: chipset_id: 0xa000
TBOOT: flags: 0x0
TBOOT: pre_production: 0
TBOOT: debug_signed: 0
TBOOT: vendor: 0x8086
TBOOT: date: 0x20091020
TBOOT: size*4: 0x85c0 (34240)
TBOOT: code_control: 0x0

```
TBOOT:      entry point: 0x00000008:00006427
TBOOT:      scratch_size: 0x8f (143)
TBOOT:      info_table:
TBOOT:          uuid: {0x7fc03aaa, 0x46a7, 0x18db, 0xac2e,
        {0x69, 0x8f, 0x8d, 0x41, 0x7f, 0x5a}}
TBOOT:              ACM_UUID_V3
TBOOT:          chipset_acm_type: 0x1 (SINIT)
TBOOT:          version: 3
TBOOT:          length: 0x28 (40)
TBOOT:          chipset_id_list: 0x4e8
TBOOT:          os_sinit_data_ver: 0x5
TBOOT:          min_mle_hdr_ver: 0x00020000
TBOOT:          capabilities: 0x0000000e
TBOOT:              rlp_wake_getsec: 0
TBOOT:              rlp_wake_monitor: 1
TBOOT:              ecx_pgtbl: 1
TBOOT:          acm_ver: 16
TBOOT:      chipset list:
TBOOT:          count: 1
TBOOT:          entry 0:
TBOOT:              flags: 0x1
TBOOT:              vendor_id: 0x8086
TBOOT:              device_id: 0xa000
TBOOT:              revision_id: 0x1
TBOOT:              extended_id: 0x0
TBOOT: SINIT's os_sinit_data version unsupported (5)
TBOOT: file addresses:
TBOOT:      &_start=00803000
TBOOT:      &_end=00878c74
TBOOT:      &_mle_start=00803000
TBOOT:      &_mle_end=00823000
TBOOT:      &_post_launch_entry=00803020
TBOOT:      &_txt_wakeup=008031f0
TBOOT:      &g_mle_hdr=0081a540
TBOOT: MLE header:
TBOOT:      uuid={0x9082ac5a, 0x476f, 0x74a7, 0x5c0f,
        {0x55, 0xa2, 0xcb, 0x51, 0xb6, 0x42}}
TBOOT:      length=34
TBOOT:      version=00020001
TBOOT:      entry_point=00000020
TBOOT:      first_valid_page=00000000
TBOOT:      mle_start_off=0
TBOOT:      mle_end_off=20000
```

```
TBOOT:      capabilities: 0x00000007
TBOOT:          rlp_wake_getsec: 1
TBOOT:          rlp_wake_monitor: 1
TBOOT:          ecx_pgtbl: 1
TBOOT: MLE start=803000, end=823000, size=20000
TBOOT: ptab_size=3000, ptab_base=00800000
TBOOT: bios_data (@77720008, 2c):
TBOOT:      version: 3
TBOOT:      bios_sinit_size: 0x0 (0)
TBOOT:      lcp_pd_base: 0x0
TBOOT:      lcp_pd_size: 0x0 (0)
TBOOT:      num_logical_procs: 4
TBOOT:      flags: 0x00000000
TBOOT: min_lo_ram: 0x0, max_lo_ram: 0x77400000
TBOOT: min_hi_ram: 0x0, max_hi_ram: 0x0
TBOOT: LCP module found
TBOOT: os_sinit_data (@77730154, 5c):
TBOOT:      version: 4
TBOOT:      mle_ptab: 0x800000
TBOOT:      mle_size: 0x20000 (131072)
TBOOT:      mle_hdr_base: 0x17540
TBOOT:      vtd_pmr_lo_base: 0x0
TBOOT:      vtd_pmr_lo_size: 0x77400000
TBOOT:      vtd_pmr_hi_base: 0x0
TBOOT:      vtd_pmr_hi_size: 0x0
TBOOT:      lcp_po_base: 0x7772014c
TBOOT:      lcp_po_size: 0x50 (80)
TBOOT:      capabilities: 0x00000002
TBOOT:          rlp_wake_getsec: 0
TBOOT:          rlp_wake_monitor: 1
TBOOT:          ecx_pgtbl: 0
TBOOT: setting MTRRs for acmod: base=77700000, size=85c0, num_pages=9
TBOOT: executing GETSEC[SENTER]...
TBOOT: ******************** TBOOT ********************
TBOOT:    unavailable
TBOOT: ***********************************************
TBOOT: command line: logging=serial,vga,memory
TBOOT: TPM is ready
TBOOT: TPM nv_locked: TRUE
TBOOT: read verified launch policy (256 bytes) from TPM NV
TBOOT: policy:
TBOOT:      version: 2
TBOOT:      policy_type: TB_POLTYPE_CONT_NON_FATAL
```

```
TBOOT:      hash_alg: TB_HALG_SHA1
TBOOT:      policy_control: 00000001 (EXTEND_PCR17)
TBOOT:      num_entries: 3
TBOOT:      policy entry[0]:
TBOOT:          mod_num: 0
TBOOT:          pcr: 18
TBOOT:          hash_type: TB_HTYPE_IMAGE
TBOOT:          num_hashes: 1
TBOOT:          hashes[0]: 75 e6 10 32 35 f4 72 3d 93 ff ed fd 3b df b6 6c 02 e2 3c 12
TBOOT:      policy entry[1]:
TBOOT:          mod_num: 1
TBOOT:          pcr: 19
TBOOT:          hash_type: TB_HTYPE_IMAGE
TBOOT:          num_hashes: 1
TBOOT:          hashes[0]: 90 c6 1f 2d 92 89 a9 ad 57 cc 36 57 79 c8 74 fb ba a1 d0 ae
TBOOT:      policy entry[2]:
TBOOT:          mod_num: 2
TBOOT:          pcr: 19
TBOOT:          hash_type: TB_HTYPE_IMAGE
TBOOT:          num_hashes: 1
TBOOT:          hashes[0]: 80 14 c6 56 fb 3d 33 ed 97 bd 08 d2 8f 35 f5 54 21 6c d4 3c
TBOOT: TPM: write nv 20000002, offset 00000000, 00000004 bytes, return = 00000002
TBOOT: Error: write TPM error: 0x2.
TBOOT: IA32_FEATURE_CONTROL_MSR: 0000ff07
TBOOT: CPU is SMX-capable
TBOOT: CPU is VMX-capable
TBOOT: SMX is enabled
TBOOT: TXT chipset and all needed capabilities present
TBOOT: TPM: write nv 20000002, offset 00000000, 00000004 bytes, return = 00000002
TBOOT: Error: write TPM error: 0x2.
TBOOT: LT.ERRORCODE=c0000001
TBOOT: AC module error : acm_type=1, progress=00, error=0
TBOOT: LT.ESTS=0
TBOOT: IA32_FEATURE_CONTROL_MSR: 0000ff07
TBOOT: CPU is SMX-capable
TBOOT: CPU is VMX-capable
TBOOT: SMX is enabled
TBOOT: TXT chipset and all needed capabilities present
TBOOT: bios_data (@77720008, 2c):
TBOOT:      version: 3
TBOOT:      bios_sinit_size: 0x0 (0)
TBOOT:      lcp_pd_base: 0x0
TBOOT:      lcp_pd_size: 0x0 (0)
```

TBOOT: num_logical_procs: 4
TBOOT: flags: 0x00000000
TBOOT: TPM: write nv 20000002, offset 00000000, 00000004 bytes, return = 00000002
TBOOT: Error: write TPM error: 0x2.
TBOOT: **measured launch succeeded**
TBOOT: bios_data (@77720008, 2c):
TBOOT: version: 3
TBOOT: bios_sinit_size: 0x0 (0)
TBOOT: lcp_pd_base: 0x0
TBOOT: lcp_pd_size: 0x0 (0)
TBOOT: num_logical_procs: 4
TBOOT: flags: 0x00000000
TBOOT: os_mle_data (@77720034, 10120):
TBOOT: version: 2
TBOOT: mbi: 0x0002cea0
TBOOT: os_sinit_data (@77730154, 5c):
TBOOT: version: 4
TBOOT: mle_ptab: 0x800000
TBOOT: mle_size: 0x20000 (131072)
TBOOT: mle_hdr_base: 0x17540
TBOOT: vtd_pmr_lo_base: 0x0
TBOOT: vtd_pmr_lo_size: 0x77400000
TBOOT: vtd_pmr_hi_base: 0x0
TBOOT: vtd_pmr_hi_size: 0x0
TBOOT: lcp_po_base: 0x7772014c
TBOOT: lcp_po_size: 0x50 (80)
TBOOT: capabilities: 0x00000002
TBOOT: rlp_wake_getsec: 0
TBOOT: rlp_wake_monitor: 1
TBOOT: ecx_pgtbl: 0
TBOOT: unsupported SINIT to MLE data version (7)
TBOOT: sinit_mle_data (@777301b0, 1f8):
TBOOT: version: 7
TBOOT: bios_acm_id:
80 00 00 00 20 09 10 07 00 00 a0 00 ff ff ff ff ff ff ff ff
TBOOT: edx_senter_flags: 0x00000000
TBOOT: mseg_valid: 0x0
TBOOT: sinit_hash:
a7 bb e6 38 df a0 20 3e be 14 c9 08 69 43 dc 48 34 97 91 ef
TBOOT: mle_hash:
f9 e1 7c f5 37 07 08 c1 83 c5 80 7d 2d 15 fa b8 c8 4c 1b e3
TBOOT: stm_hash:
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

```
TBOOT:      lcp_policy_hash:
    08 b3 27 51 a4 52 21 c5 db 45 15 a9 ae 2e ff f9 f8 df e5 8f
TBOOT:      lcp_policy_control: 0x00000000
TBOOT:      rlp_wakeup_addr: 0x77701d10
TBOOT:      num_mdrs: 7
TBOOT:      mdrs_off: 0x98
TBOOT:      num_vtd_dmars: 184
TBOOT:      vtd_dmars_off: 0x140
TBOOT:      sinit_mdrs:
TBOOT:          0000000000000000 - 00000000000a0000 (GOOD)
TBOOT:          0000000000100000 - 0000000000f00000 (GOOD)
TBOOT:          0000000001000000 - 0000000077700000 (GOOD)
TBOOT:          0000000000000000 - 0000000000000000 (GOOD)
TBOOT:          0000000000000000 - 0000000000000000 (GOOD)
TBOOT:          0000000077800000 - 0000000078000000 (SMRAM NON-OVERLAY)
TBOOT:          00000000e0000000 - 00000000f0000000 (PCIE EXTENDED CONFIG)
TBOOT: RSDP (v002 HPQOEM) @ 0x000f2b20
TBOOT: Seek in XSDT...
TBOOT: entry[0] sig = FACP @ 0x773fc000
TBOOT: entry[1] sig = HPET @ 0x773fb000
TBOOT: entry[2] sig = APIC @ 0x773fa000
TBOOT: acpi_table_ioapic @ 773fa06c, .address = fec00000
TBOOT: RSDP (v002 HPQOEM) @ 0x000f2b20
TBOOT: Seek in XSDT...
TBOOT: entry[0] sig = FACP @ 0x773fc000
TBOOT: entry[1] sig = HPET @ 0x773fb000
TBOOT: entry[2] sig = APIC @ 0x773fa000
TBOOT: entry[3] sig = MCFG @ 0x773f9000
TBOOT: acpi_table_mcfg @ 773f9000, .base_address = e0000000
TBOOT: mtrr_def_type: e = 1, fe = 1, type = 0
TBOOT: mtrrs:
TBOOT:          base     mask    type     v
TBOOT:          0ffc00   fffc00  05       1
TBOOT:          000000           f80000 06       1
TBOOT:          078000ff8000  00       1
TBOOT:          000000           000000          00       0
TBOOT:          000000           000000          00       0
TBOOT:          000000           000000          00       0
TBOOT:          000000           000000          00       0
TBOOT:          000000           000000          00       0
TBOOT: min_lo_ram: 0x0, max_lo_ram: 0x77400000
TBOOT: min_hi_ram: 0x0, max_hi_ram: 0x0
TBOOT: MSR for SMM monitor control on ILP 0 is 0x0.
```

```
TBOOT: verifying ILP is opt-out or has the same MSEG header with TXT.MSEG.BASE
          opt-out
TBOOT:  : succeeded.
TBOOT: enabling SMIs on BSP
TBOOT: mle_join.entry_point = 8031f0
TBOOT: mle_join.seg_sel = 8
TBOOT: mle_join.gdt_base = 804000
TBOOT: mle_join.gdt_limit = 3f
TBOOT: joining RLPs to MLE with MONITOR wakeup
TBOOT: rlp_wakeup_addr = 0x77701d10
TBOOT: cpu 4 waking up from TXT sleep
TBOOT: waiting for all APs (3) to enter wait-for-sipi...
TBOOT: MSR for SMM monitor control on RLP(4) is 0x0
TBOOT: verifying ILP's MSR_IA32_SMM_MONITOR_CTL with RLP(4)'s
      : succeeded.
TBOOT: enabling SMIs on cpu 4
TBOOT: .VMXON done for cpu 4
TBOOT:
TBOOT: cpu 5 waking up from TXT sleep
TBOOT: launching mini-guest for cpu 4
TBOOT: MSR for SMM monitor control on RLP(5) is 0x0
TBOOT: verifying ILP's MSR_IA32_SMM_MONITOR_CTL with RLP(5)'s
      : succeeded.
TBOOT: enabling SMIs on cpu 5
TBOOT: VMXON done for cpu 5
TBOOT: launching mini-guest for cpu 5
TBOOT: cpu 1 waking up from TXT sleep
TBOOT: MSR for SMM monitor control on RLP(1) is 0x0
TBOOT: .verifying ILP's MSR_IA32_SMM_MONITOR_CTL with RLP(1)'s
     . : succeeded.
TBOOT: enabling SMIs on cpu 1
TBOOT: .VMXON done for cpu 1
TBOOT: launching mini-guest for cpu 1
TBOOT: .
TBOOT: all APs in wait-for-sipi
TBOOT: saved IA32_MISC_ENABLE = 0x00850089
TBOOT: set LT.CMD.SECRETS flag
TBOOT: opened TPM locality 1
TBOOT: TPM: write nv 20000002, offset 00000000, 00000004 bytes, return = 00000002
TBOOT: Error: write TPM error: 0x2.
TBOOT: RSDP (v002 HPQOEM) @ 0x000f2b20
TBOOT: Seek in XSDT...
TBOOT: entry[0] sig = FACP @ 0x773fc000
```

```
TBOOT: entry[1] sig = HPET @ 0x773fb000
TBOOT: entry[2] sig = APIC @ 0x773fa000
TBOOT: entry[3] sig = MCFG @ 0x773f9000
TBOOT: entry[4] sig = TCPA @ 0x773f7000
TBOOT: entry[5] sig = SSDT @ 0x773d4000
TBOOT: entry[6] sig = SSDT @ 0x773d3000
TBOOT: entry[7] sig = SLIC @ 0x773d2000
TBOOT: entry[8] sig = DMAR @ 0x773d1000
TBOOT: DMAR table @ 0x773d1000 saved.
TBOOT: original e820 map:
TBOOT:      0000000000000000 - 000000000009fc00  (1)
TBOOT:      000000000009fc00 - 00000000000a0000  (2)
TBOOT:      00000000000ef000 - 0000000000100000  (2)
TBOOT:      0000000000100000 - 00000000771ab000  (1)
TBOOT:      00000000771ab000 - 00000000771b3000  (2)
TBOOT:      00000000771b3000 - 00000000771b9000  (1)
TBOOT:      00000000771b9000 - 0000000077229000  (2)
TBOOT:      0000000077229000 - 0000000077294000  (1)
TBOOT:      0000000077294000 - 000000007729a000  (2)
TBOOT:      000000007729a000 - 00000000772bf000  (1)
TBOOT:      00000000772bf000 - 00000000772cf000  (2)
TBOOT:      00000000772cf000 - 000000007730d000  (4)
TBOOT:      000000007730d000 - 000000007730e000  (3)
TBOOT:      000000007730e000 - 00000000773cf000  (4)
TBOOT:      00000000773cf000 - 00000000773ff000  (3)
TBOOT:      00000000773ff000 - 0000000077400000  (1)
TBOOT:      0000000077400000 - 0000000077800000  (2)
TBOOT:      0000000077800000 - 0000000078000000  (2)
TBOOT:      00000000e0000000 - 00000000f0000000  (2)
TBOOT:      00000000fec00000 - 00000000fec01000  (2)
TBOOT:      00000000fed10000 - 00000000fed14000  (2)
TBOOT:      00000000fed19000 - 00000000fed1a000  (2)
TBOOT:      00000000fed1b000 - 00000000fed1c000  (2)
TBOOT:      00000000fed1c000 - 00000000fed20000  (2)
TBOOT:      00000000fee00000 - 00000000fee01000  (2)
TBOOT:      00000000ffd00000 - 0000000100000000  (2)
TBOOT: verifying module 0 of mbi (87a000 - 999873) in e820 table
     (range from 000000000087a000 to 0000000000999874 is in E820_RAM)
TBOOT: : succeeded.
TBOOT: verifying module 1 of mbi (99a000 - 1153127) in e820 table
     (range from 000000000099a000 to 0000000001153128 is in E820_RAM)
TBOOT: : succeeded.
TBOOT: verifying module 2 of mbi (1154000 - 18ebdff) in e820 table
```

```
    (range from 0000000001154000 to 00000000018ebe00 is in E820_RAM)
TBOOT: : succeeded.
TBOOT: verifying module 3 of mbi (18ec000 - 18f45bf) in e820 table
    (range from 00000000018ec000 to 00000000018f45c0 is in E820_RAM)
TBOOT: : succeeded.
TBOOT: verifying module 4 of mbi (18f5000 - 18f504f) in e820 table
    (range from 00000000018f5000 to 00000000018f5050 is in E820_RAM)
TBOOT: : succeeded.
TBOOT: protecting TXT heap (77720000 - 777fffff) in e820 table
TBOOT: protecting SINIT (77700000 - 7771ffff) in e820 table
TBOOT: protecting TXT Private Space (fed20000 - fed2ffff) in e820 table
TBOOT: verifying e820 table against SINIT MDRs: verification succeeded.
TBOOT: TPM: write nv 20000002, offset 00000000, 00000004 bytes, return = 00000002
TBOOT: Error: write TPM error: 0x2.
TBOOT: verifying tboot and its page table (800000 - 878c73) in e820 table
    (range from 0000000000800000 to 0000000000878c74 is in E820_RAM)
TBOOT: : succeeded.
TBOOT: protecting tboot (800000 - 878fff) in e820 table
TBOOT: reserving tboot memory log (60000 - 67fff) in e820 table
TBOOT: adjusted e820 map:
TBOOT:      0000000000000000 - 0000000000060000  (1)
TBOOT:      0000000000060000 - 0000000000068000  (2)
TBOOT:      0000000000068000 - 000000000009fc00  (1)
TBOOT:      000000000009fc00 - 00000000000a0000  (2)
TBOOT:      00000000000ef000 - 0000000000100000  (2)
TBOOT:      0000000000100000 - 0000000000800000  (1)
TBOOT:      0000000000800000 - 0000000000879000  (5)
TBOOT:      0000000000879000 - 0000000000f00000  (1)
TBOOT:      0000000000f00000 - 0000000001000000  (2)
TBOOT:      0000000001000000 - 00000000771ab000  (1)
TBOOT:      00000000771ab000 - 00000000771b3000  (2)
TBOOT:      00000000771b3000 - 00000000771b9000  (1)
TBOOT:      00000000771b9000 - 0000000077229000  (2)
TBOOT:      0000000077229000 - 0000000077294000  (1)
TBOOT:      0000000077294000 - 000000007729a000  (2)
TBOOT:      000000007729a000 - 00000000772bf000  (1)
TBOOT:      00000000772bf000 - 00000000772cf000  (2)
TBOOT:      00000000772cf000 - 000000007730d000  (4)
TBOOT:      000000007730d000 - 000000007730e000  (3)
TBOOT:      000000007730e000 - 00000000773cf000  (4)
TBOOT:      00000000773cf000 - 00000000773ff000  (3)
TBOOT:      00000000773ff000 - 0000000077400000  (1)
TBOOT:      0000000077400000 - 0000000077700000  (2)
```

TBOOT: 0000000077700000 - 0000000077720000 (2)
TBOOT: 0000000077720000 - 0000000077800000 (2)
TBOOT: 0000000077800000 - 0000000078000000 (2)
TBOOT: 00000000e0000000 - 00000000f0000000 (2)
TBOOT: 00000000fec00000 - 00000000fec01000 (2)
TBOOT: 00000000fed10000 - 00000000fed14000 (2)
TBOOT: 00000000fed19000 - 00000000fed1a000 (2)
TBOOT: 00000000fed1b000 - 00000000fed1c000 (2)
TBOOT: 00000000fed1c000 - 00000000fed20000 (2)
TBOOT: 00000000fed20000 - 00000000fed30000 (2)
TBOOT: 00000000fee00000 - 00000000fee01000 (2)
TBOOT: 00000000ffd00000 - 0000000100000000 (2)
TBOOT: TPM: write nv 20000002, offset 00000000, 00000004 bytes, return = 00000002
TBOOT: Error: write TPM error: 0x2.
TBOOT: **verifying module "/xen-3.4.gz iommu=required"...**
TBOOT: **OK : 75 e6 10 32 35 f4 72 3d 93 ff ed fd 3b df b6 6c 02 e2 3c 12**
TBOOT: TPM: write nv 20000002, offset 00000000, 00000004 bytes, return = 00000002
TBOOT: Error: write TPM error: 0x2.
TBOOT: **verifying module "/vmlinuz-2.6.18.8-xen ro root=LABEL=/1 rhgb"...**
TBOOT: **OK : 90 c6 1f 2d 92 89 a9 ad 57 cc 36 57 79 c8 74 fb ba a1 d0 ae**
TBOOT: TPM: write nv 20000002, offset 00000000, 00000004 bytes, return = 00000002
TBOOT: Error: write TPM error: 0x2.
TBOOT: **verifying module "/initrd-2.6.18.8-xen.img"...**
TBOOT: **OK : 80 14 c6 56 fb 3d 33 ed 97 bd 08 d2 8f 35 f5 54 21 6c d4 3c**
TBOOT: TPM: write nv 20000002, offset 00000000, 00000004 bytes, return = 00000002
TBOOT: Error: write TPM error: 0x2.
TBOOT: policy entry for module 3 not found
TBOOT: TPM: write nv 20000002, offset 00000000, 00000004 bytes, return = 00000002
TBOOT: Error: write TPM error: 0x2.
TBOOT: modules in mbi but not in policy.
TBOOT: policy entry for module 4 not found
TBOOT: TPM: write nv 20000002, offset 00000000, 00000004 bytes, return = 00000002
TBOOT: Error: write TPM error: 0x2.
TBOOT: modules in mbi but not in policy.
TBOOT: all modules are verified
TBOOT: pre_k_s3_state:
TBOOT: vtd_pmr_lo_base: 0x0
TBOOT: vtd_pmr_lo_size: 0x77400000
TBOOT: vtd_pmr_hi_base: 0x0
TBOOT: vtd_pmr_hi_size: 0x0
TBOOT: pol_hash: 63 2f b6 06 cd 4d e5 8e 64 2a d8 a9 f7 33 46 95 4d 23 ec 2e
TBOOT: VL measurements:
TBOOT: PCR 17: 7c b2 7c 30 1c b6 80 70 b8 0f 7e 57 71 f7 6f 9a f7 ae 91 61

TBOOT: PCR 18: 75 e6 10 32 35 f4 72 3d 93 ff ed fd 3b df b6 6c 02 e2 3c 12
TBOOT: **PCR 18**: 75 e6 10 32 35 f4 72 3d 93 ff ed fd 3b df b6 6c 02 e2 3c 12
TBOOT: **PCR 19**: 90 c6 1f 2d 92 89 a9 ad 57 cc 36 57 79 c8 74 fb ba a1 d0 ae
TBOOT: **PCR 19**: 80 14 c6 56 fb 3d 33 ed 97 bd 08 d2 8f 35 f5 54 21 6c d4 3c
TBOOT: PCRs before extending:
TBOOT: PCR 17: f9 e2 11 49 6c 35 61 5e b8 e1 a9 1a e0 ed 4a 62 42 e2 ec 5e
TBOOT: PCR 18: e8 4f 85 88 fc d6 9c eb ca 81 ad db 0d 2c 78 b0 7e a3 ab 20
TBOOT: PCRs after extending:
TBOOT: PCR 17: 53 03 7e c2 5c 23 41 1e e5 c5 ee b3 5a 91 a4 fe a3 8c 0c 08
TBOOT: PCR 18: 8f 9b f0 01 0f 96 e8 7b aa 78 a8 93 05 01 29 4e 39 24 f6 60
TBOOT: tboot_shared data:
TBOOT: version: 5
TBOOT: log_addr: 0x00060000
TBOOT: shutdown_entry: 0x008031b0
TBOOT: shutdown_type: 0
TBOOT: tboot_base: 0x00803000
TBOOT: tboot_size: 0x75c74
TBOOT: num_in_wfs: 3
TBOOT: checking whether module 4 is an SINIT AC module...
TBOOT: ACM size is too small: acmod_size=50, sizeof(acm_hdr)=4
TBOOT: : failed.
TBOOT: checking whether module 3 is an SINIT AC module...
TBOOT: : succeeded.
TBOOT: user-provided SINIT found: /sinit.bin
TBOOT: LCP module found
TBOOT: kernel is ELF format
TBOOT: transfering control to kernel @0x00100000...
TBOOT: VMXOFF done for cpu 1
TBOOT: cpu 1 waking up, SIPI vector=8c000
TBOOT: VMXOFF done for cpu 4
TBOOT: cpu 4 waking up, SIPI vector=8c000
TBOOT: VMXOFF done for cpu 5
TBOOT: cpu 5 waking up, SIPI vector=8c000

For more information

HP Technology Center http://www.hp.com/go/techcenter

Intel's Trusted eXecution Technology Home Page
http://www.intel.com/technology/security/

Trusted Boot Home Page http://sourceforge.net/projects/tboot

Trusted Boot Source http://www.bughost.org/repos.hg/tboot.hg/

HP Product Number: 644342-001

April 2009