

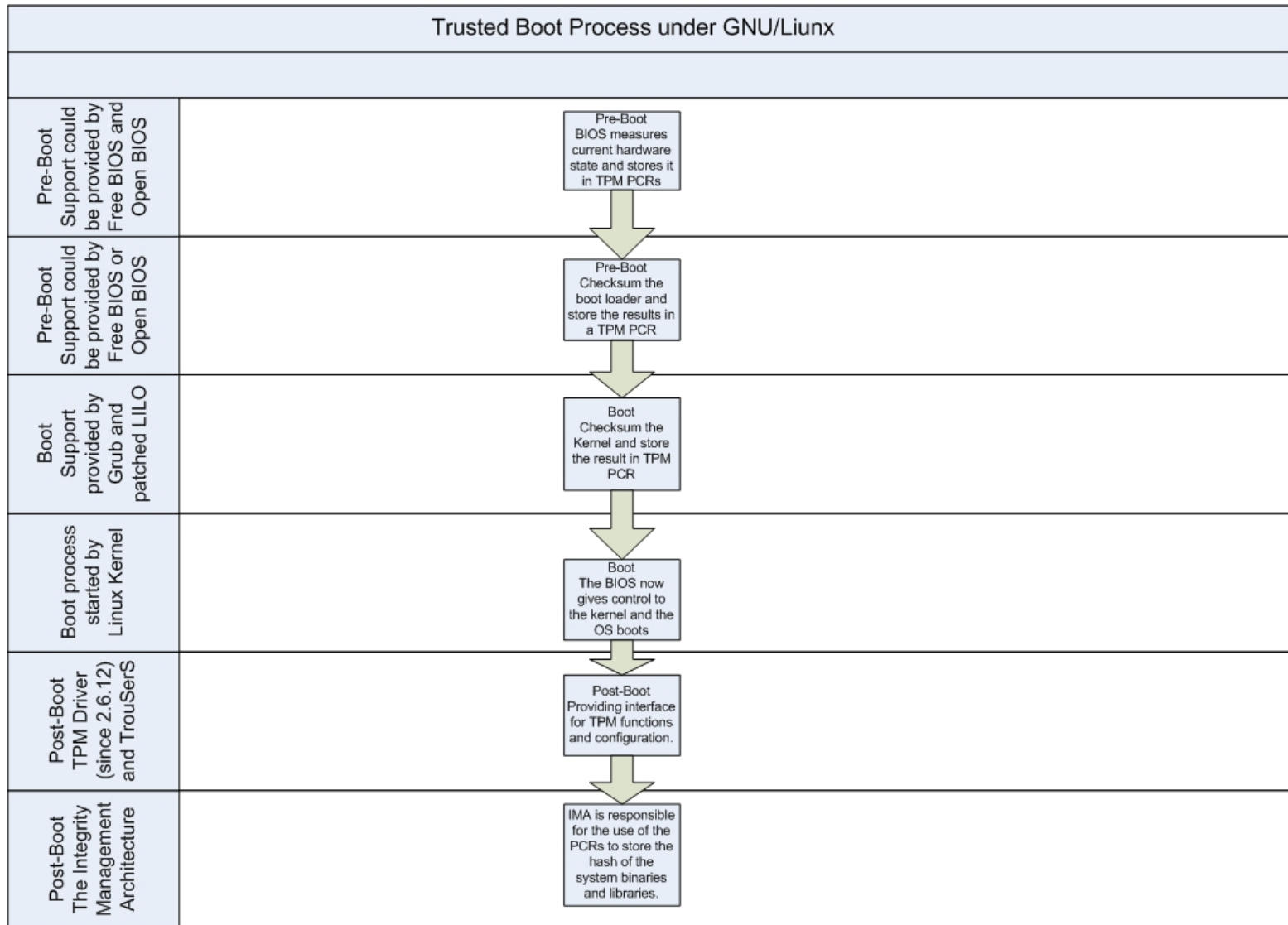
Trusted Computing Support  
in  
GNU/Linux Operating System

By,

Chaitanya Vinay Hazarey

Submitted for the CSCI 599tc Trusted Computing Course

# Components of GNU/Linux at each stage of Trusted Boot Process



# BIOS Support

---

- BIOS support is necessary for the “measurement” of the hardware of the system.
- It is also supposed to support the hashing and extending of the Master Boot Record.
- These measurements of the hardware and MBR are extended in the Platform Configuration Register (PCR).
- It is possible to support this operations in the BIOS by implementing them with Free-BIOS (Linux-BIOS) or Open-BIOS.
- Currently these types of operations are not supported by these BIOS's.

# Boot Loader Support

---

- The boot loader should be capable of measuring the OS kernel and extending the value to a PCR.
- Grub has patches to support Trusted Computing and Trusted Boot compliant with the TCG 1.1b specifications.
- LILO has a downloadable version of LILO called the LILO w/TCPA Support available from Enforcer Linux Security Module (LSM) site.
- Both these measure and extend the configuration files and the initial stages of the boot-loader.
- Then they continue the measurement and extension of the following stages as the boot process proceeds.

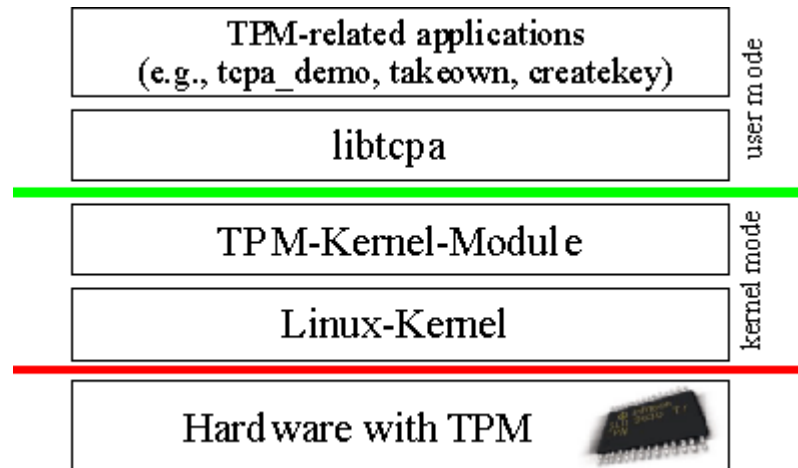
# How does it do it ?

---

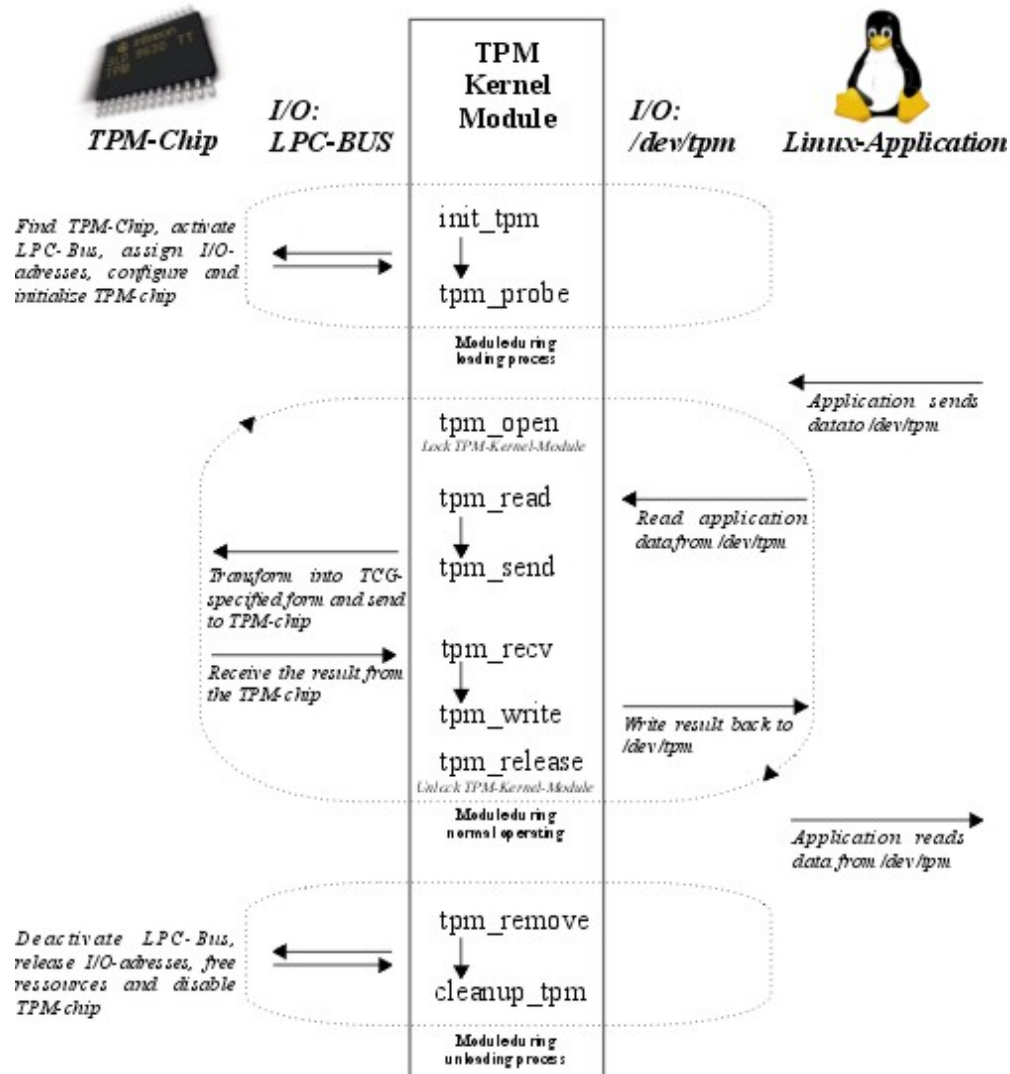
- Grub takes measurements during the process of loading Grub.
- Stage 1 (MBR) Measured by the BIOS itself.
- Stage 1.5 measures the first sector of the stage 2.
- The first stage of the stage 1.5 measures the remaining sectors.
- After the successful boot of Grub, it measures the grub.conf file and then proceeds to measure the files specified in the grub.conf file.

# TPM Driver

- Information is specific to the Infineon Chip drivers → libtpm driver
- Currently supports Infineon SLD 9630 TT 1.1 and Infineon SLB 9635 1.2 TPMs.
- Placement of the driver:



# TPM Driver Operation Details



# TPM Driver Operation Details

---

- Kernel and User level processes converse with the TPM using the special character node devices under `/dev/tpm` file system.
- IBM provides a library called `libtpm` to converse with the chips according to the TCG specifications.
- The interface between the TPM and the processes is a Linux Kernel Module → `tpm_infineon.ko`
- The Kernel module will read the data from the `/dev/tpm` transforms it to a TCG Specs. And sends it to the TPM which stores it in its FIFO.
- TPM performs the requested operations and then sends the results back to the LKM which in turn writes it to the `/dev/tpm` interface.

# TrouSerS

---

- User space activities for TPM driver is handled by the TrouSerS (TSS) Stack.
- TSS API provide the following functions:
  - RSA key pair generation
  - RSA encryption and decryption using PKCS v1.5 and OAEP padding
  - RSA sign/verify
  - Extend data into the TPM's PCRs and log these events
  - Seal data to arbitrary PCRs
  - Random Number Generation
  - RSA key storage
- TSS does not comply completely with the TCG Specs, but can be configured to be strictly compliant.

# The Integrity Management Architecture

---

- IMA is responsible for the use of the PCRs to store the hash of the system binaries and libraries.
- Extended Verification Module (EVM) provides the measurements
- Simple Linux Integrity Module (SLIM) identifies all the executables and the configuration files on the system.
- IMA can perform several of the critical functions of TCG such as Remote Attestation and Secure Data Storage.
- Example from the IBM slides:

```
# cat /sys/kernel/security/ima/ascii_runtime_measurements
```

```
10 1ac2616d0a992514d02c69ba1e2cfde6e9096fce boot_aggregate
10 668a6a23db3b47ffd229f3642ab8b86d00000000 /sbin/init
10 e78baf9c4cf6accebc7ce36891a9238a00000000 /lib/ld-2.3.4.so
10 3b21b2c293b97b231edc89a34f02593300000000
/etc/ld.so.cache
```

Sources: [http://www.research.ibm.com/gsal/tcpa/TCFL-TPM\\_intro.pdf](http://www.research.ibm.com/gsal/tcpa/TCFL-TPM_intro.pdf)  
[http://www.usenix.org/events/sec04/tech/full\\_papers/sailer/sailer\\_html/](http://www.usenix.org/events/sec04/tech/full_papers/sailer/sailer_html/)  
[http://domino.research.ibm.com/comm/research\\_projects.nsf/pages/ssd\\_ima.index.html](http://domino.research.ibm.com/comm/research_projects.nsf/pages/ssd_ima.index.html)  
<http://lwn.net/Articles/137306/>

# Trusted Computing and GNU/Linux a perspective

---

- Support for the TCG Specifications and the TPM in GNU/Linux operating system have come a long way since their introduction.
- The use of TC in Open Source Operating systems will according to me, be instrumental in increasing their popularity and acceptance as a “Trustworthy” alternative.
- The use of TC in an Open Source box does not limit the “hacking” ability of the owner but does limit his “cracking” ability.
- The implementation of the TCG Specifications as they are now, and the proposal of a “Trusted Computer” should be certainly evaluated and remodeled to include support for separate “domains” depending upon the choice of the user or the enforcer.
- In conclusion inclusion of support for TC in GNU/Linux will be a step forward in the maturing of GNU/Linux into a more mature, secure and reliable operating system.

# References

---

1. <http://lwn.net/Articles/144681/>
2. [http://www.usenix.org/events/sec04/tech/full\\_papers/sailer/sailer\\_html/](http://www.usenix.org/events/sec04/tech/full_papers/sailer/sailer_html/)
3. [http://domino.research.ibm.com/comm/research\\_projects.nsf/pages/ssd\\_ima.index.html](http://domino.research.ibm.com/comm/research_projects.nsf/pages/ssd_ima.index.html)
4. <http://trousers.sourceforge.net/faq.html>
5. <http://trousers.sourceforge.net/>
6. [http://www.prosec.rub.de/tpm/tpm\\_driver\\_details.html](http://www.prosec.rub.de/tpm/tpm_driver_details.html)
7. [http://www.research.ibm.com/gsal/tcpa/TCFL-TPM\\_intro.pdf](http://www.research.ibm.com/gsal/tcpa/TCFL-TPM_intro.pdf)
8. <http://lwn.net/Articles/137306/>
9. [http://www.research.ibm.com/gsal/tcpa/TCFL-TPM\\_intro.pdf](http://www.research.ibm.com/gsal/tcpa/TCFL-TPM_intro.pdf)
10. [https://www.cypherpunks.to/TCPA\\_DEFCON\\_10.pdf](https://www.cypherpunks.to/TCPA_DEFCON_10.pdf)
11. <http://trousers.sourceforge.net/grub.html>
12. [http://openbios.info/Welcome\\_to\\_OpenBIOS](http://openbios.info/Welcome_to_OpenBIOS)
13. <http://freebios.sourceforge.net/>
14. [http://www.linuxbios.org/Welcome\\_to\\_LinuxBIOS](http://www.linuxbios.org/Welcome_to_LinuxBIOS)