

# Knoppix 5.1.1 for Trusted Computing Geeks



National Institute of  
Advanced Industrial Science  
and Technology  
**AIST**

**CRTM/TCGBIOS**

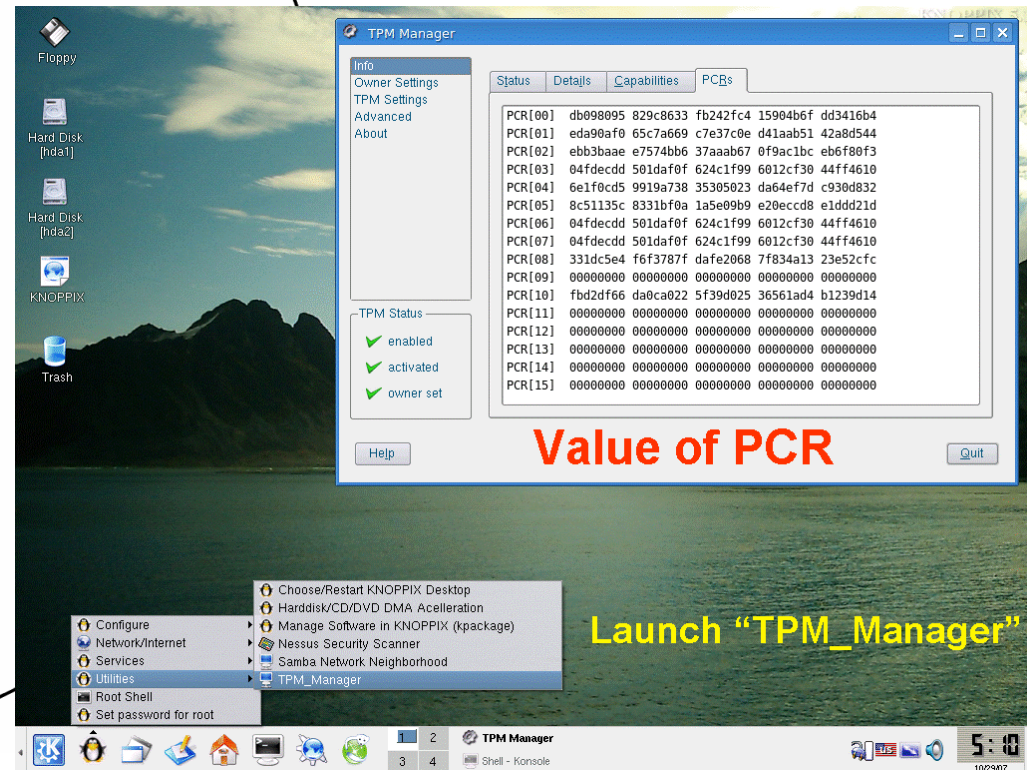
*Chain of Trust*

↳ **Grub-IMA 1.1.0.0**

↳ **Linux-IMA 2.6.19**

↳ **TrouSerS 0.2.9.1**

↳ **TPM Manager 0.4**



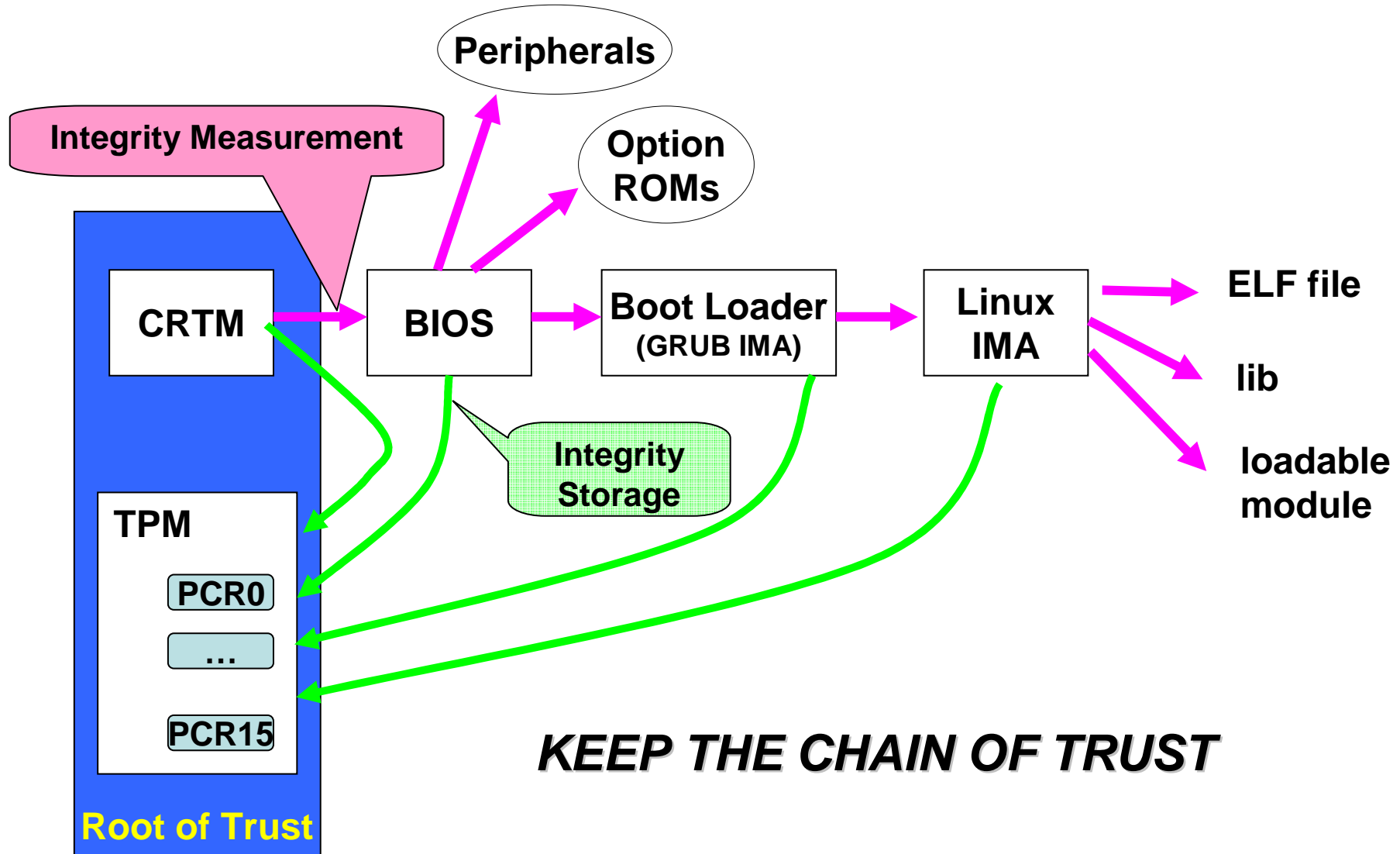
ISO file will be downloadable  
<http://unit.aist.go.jp/itri/knoppix/index-en.html>

AIST  
Kuniyasu Suzuki

# Trusted Computing

- Defined by TCG (Trusted Computing Groups)
  - <https://www.trustedcomputinggroup.org>
  - Member: AMD, HP, IBM, Infineon, Intel, Lenovo, Microsoft, SUN, etc
  - Security Chip “**TPM**” (Trusted Platform Module) and “**CTRM**” (Core Root of Trust Measurement) are Root of Trust of Platform.
  - Trusted Boot measures and logs files before they are used. The measurement is kept in a register in TPM.
- The CD shows dynamic change of registers (PCR: Platform Configuration Register) in a TPM.

# Trusted Boot



# Log of Trusted Boot

– /sys/kernel/security/tpm0/ascii\_bios\_measurements

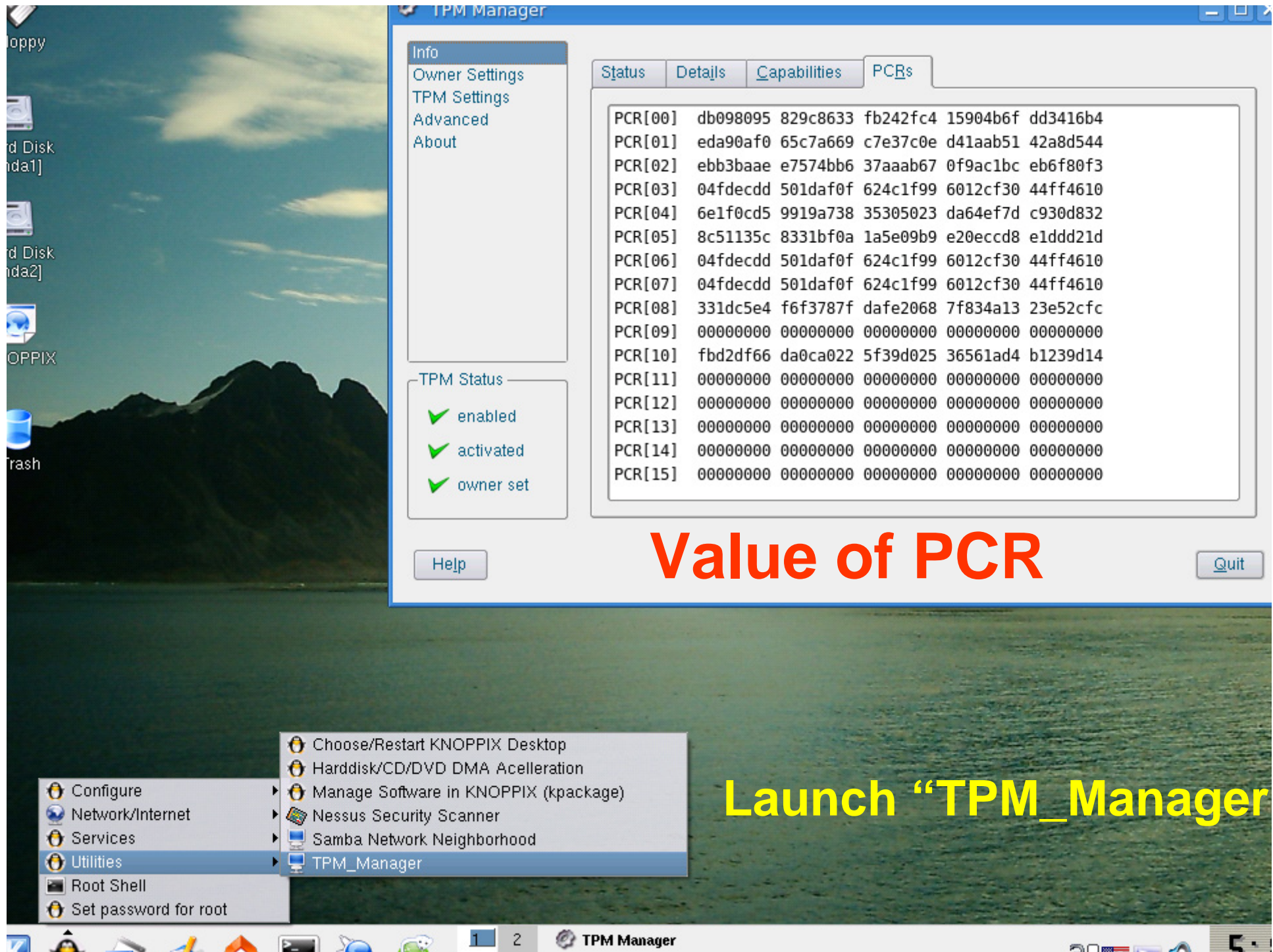
PCR	SHA1	Event
↓	↓	↓
5	d9be6524a5f5047db5866813acf3277892a7a30a	04 [ ]
6	d9be6524a5f5047db5866813acf3277892a7a30a	04 [ ]
7	d9be6524a5f5047db5866813acf3277892a7a30a	04 [ ]
4	38f30a0a967fcf2bfee1e3b2971de540115048c8	05 [Returned INT 19h]
4	89f0284e00992d067654818a9f2c09bbaa31acde	05 [Bootimg CD ROM, - MATSHITADVD-RAM UJ-833S]
4	8dfd8ee51758ac29ccf1bb6eedc2d483acf83a9b	0d [IPL] <a href="#">block[0x18800-0x189FF] on CD-ROM</a>
4	1cdac212c5342627905cfcc4931972a8b4a09996	0d [IPL] <a href="#">/boot/grub/stage2_eltorito</a>
4	2cedbf54913d69d027c5b97e02763f921b16e345	06 [ ]
4	8cdc27ec545eda33fbba1e8b8dae4da5c7206972	04 [Grub Event Separator]
5	8cdc27ec545eda33fbba1e8b8dae4da5c7206972	04 [Grub Event Separator]
5	f1f74d078d57197ee9cd9205995a6ba5e6a68cbf	0e [IPL Partition Data] <a href="#">/boot/grub/grub.conf</a>
5	aed235d4ddb5fed00156f4991f2c1d1330c97694	1105 [ ]
8	94c417906f8d383b811d918dce6bafdbc650ed42	1205 [ ] <a href="#">/boot/isolinux/linux-ima</a>
8	793eb4a591229afe35d60d5c2b66cee9dc33225c	1405 [ ] <a href="#">/boot/isolinux/minirt-ima.gz</a>
5	2431ed60130faeaf3a045f21963f71cacd46a029	04 [OS Event Separator]
8	2431ed60130faeaf3a045f21963f71cacd46a029	04 [OS Event Separator]
8	fac33a1fc0ad42c07d00322d64c23f67567f334a	1005 [ ]

**Measured blocks, Measured files**

# Log of Linux IMA

– /sys/kernel/security/ima/ascii\_runtime\_measurements

PCR	SHA1	Event
↓	↓	↓
10 eeb9e57fc3a66e85858585329c7291a2e138d695		boot_aggregate
10 4cd410cbd7766b0672dfcb0b73756c490c1262b6		/static/ash
10 449c076c8bbde638c37e075d63ccd7a6ac6602a0		/static/instrmod
10 06dd0a423bd7d35ea2388c481a329b34552db3c0		pas16
10 23a1ba028254b2d5c14f7d6240764706f83bcaa9		psi240i
10 0fa2ec2a67a3e33ea062f4715b1a0d566fe5ce83		t128
10 b55dfa9b2ab368b7f2d839b39dd69613c69a0d56		u14_34f
10 c68b8de398d26abf41989364eb77be153464cd87		wd7000
10 cccf8dc1ff3748dcfa8c4d145a461a3deda6431d		usbcore
10 0a2447092eb5d5b337cccf2afb75dcdac7c40de		ehci_hcd
10 bbaa6a8dfb5fe4046c4dec4b6d3d98db15067491		uhci_hcd
10 ed884c4117228e62e1308d66c7d874eecbf37c49		ohci_hcd
10 28a42c13e7f1a184c5942504f4212df6bf486d9b		libusual
10 da56881b1a67e4fc77c435fa707bb7a0d965b9dd		ff_memless
10 60a55c22343bfcf36cdb1ad29f821766ec0d7434		usbhid
10 e77e0f18af3926c57a9d670af1bf9b1bf6c74664		usb_storage
10 b8e66d764704d0d743676ab58679366a178e07e2		ieee1394
10 b2242bc1f7ffa3f8d796061f3098cd0a9f1b5690		ohci1394
10 6a32e816d63e3c36b652087309f11a78459ab3d5		sbp2
10 00646e8ef195e2c8646a0988fbd08c3e2085c9da		/static/ntfs-3g
10 0bdf9cd0d0f7378a9a52731691dbda035f6f47ed		cloop
10 e3ed81fdceb12c09d7871ecec464b915b3e1c12		/KNOPPIX/bin/lm



# How to Use

- Setup TPM Enable on the BIOS.
- Boot from CD. Select “knoppix (2.6.19+ima)” at GRUB Menu.
- Run “tpmmager”
  - From command line  
\$ sudo tpmmanager
  - From KDE Menu  
KNOPPIX->Utilities -> TPM\_Manager
- Move to “PCRs” tabs on TPM Manger
  - Run applications. You will confirm the change of PCR[10].
  - PCR[10] is changed by Linux-IMA when ELF, lib, and loadable module files are opened.
- Logs
  - Linux-IMA  
**/sys/kernel/security/ima/ascii\_bios\_measurements**
  - GRUB-IMA  
**/sys/kernel/security/tpm0/ascii\_runtime\_measurements**
  - If you can not find these files, mount the directory.  
**# mount -t securityfs none /sys/kernel/security**

# Confirmed PC

- ThinkPAD X30, T42
  - TPM: Atmel 1.1b
- LetsNote Y7
  - TPM: Infineon
- Please tell us PC name when you confirm.

[k.suzaki@aist.go.jp](mailto:k.suzaki@aist.go.jp)

# Included Tools

- GRUB-IMA developed by IBM Research
  - <http://trousers.sourceforge.net/grub.html>
- Linux-IMA (Integrity Measurement Architecture) developed by IBM Research
  - <http://sourceforge.net/projects/linux-ima>
- TrouSerS developed by IBM/LTC
  - <http://trousers.sourceforge.net/>
- TPM Manager developed by C. Stueble and A. Zaerin
  - <http://sourceforge.net/projects/tpmmanager>

## **Acknowledgement**

This study has been sponsored by the Ministry of Economy, Trade and Industry, Japan (METI) under contract, New-generation Information Security R&D Program.