VMKnoppix 20080827 (based on KNOPPPIX5.3.1 DVD size)

VMKnoppix is 1DVD Linux(KNOPPIX) which includes a lot of virtual machine software.

This is security enhanced version.

http://www.rcis.aist.go.jp/project/knoppix/vmknoppix/index-en.html

■ Special Features

- **Virtual TPM** becomes effective on Xen and KVM/QEMU. The virtual machines are used for Trusted Computing..
- The **LiveCD of trusted computing** (GRUB-IMA, Linux-IMA kernel, TrouSerS, and OpenPTS) which was called "KNOPPIX for Trusted Computing Geeks" is included.
- **TPM Checker** which shows the status of TPM is included.
- **FailSave-C**, **vx32**, and **LLVM(Low Level Virtual Machine)**, which are the compiler for security and dynamic optimization, are included.
- Secure virtual machine monitor **"BitVisor"** is updated to 0.3.
- Include Internet boot loader **"InetBoot".**
  - The GRUB Menu includes items of InetBoot for old VMKnoppix/Xenoppix.
- Includes network bootloader "**gPXE"** which deals with normal PXE and HTTP/iSCSI boot.
- Include Internet Client **"OS Circular"**.
  - It enables to boot some Linux Distributions {CentOS5 |Debian Etch| Ubuntu606 |Ubuntu610 |Ubuntu704} on a virtual machine {Xen|QEMU|KQEMU|KVM} with Internet Virtual Disk "Trusted HTTP-FUSE CLOOP".

VMKnoppix includes the following virtual machine software.

- **Xen3.2.1 (Dom0 kernel 2.6.18)** http://www.cl.cam.ac.uk/research/srg/netos/xen/
- **BitVisor0.3** http://www.securevm.org/bitvisor.html (Written in Japanese)
- **KVM60** http://sourceforge.net/projects/kvm
- **QEMU091** http://fabrice.bellard.free.fr/qemu/
- **KQEMU** http://fabrice.bellard.free.fr/qemu/kqemu-doc.html
- **UML** http://user-mode-linux.sourceforge.net/
- **Virtual Box** http://www.virtualbox.org/

VMKnoppix includes the following network boot software.

- **gPXE** http://www.etherboot.org
- **InetBoot** http://openlab.jp/oscircular/inetboot/
- **OSCircular** http://openlab.jp/oscircular

VMKnoppix includes the following compilers for security and optimization

- **FailSafe-C** http://www.rcis.aist.go.jp/project/FailSafeC-ja.html
- **VX32** http://pdos.csail.mit.edu/~baford/vm/
- **LLVM** http://llvm.org/

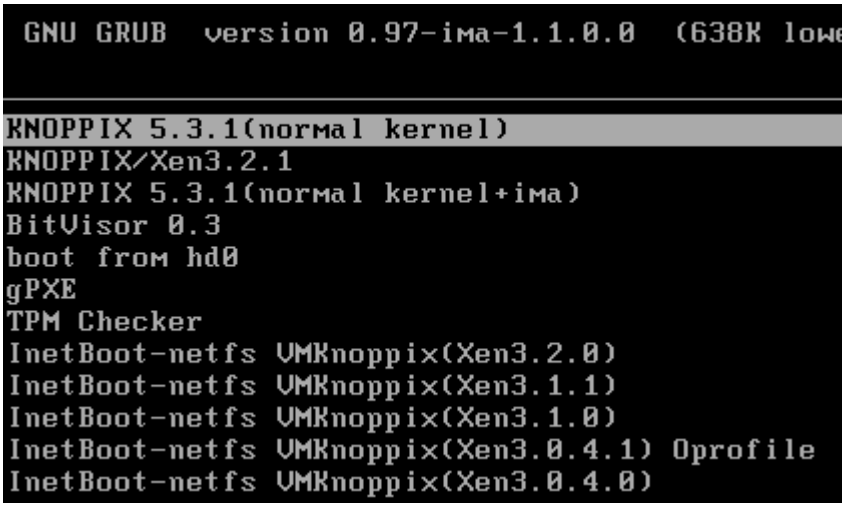
Download

- File Name: knoppix_v5.3.1DVD20080326_xen3.2.1-20080827.iso (MD5: bdf1ef34a688cef1e378919acbedccdf)
- FTP: (Ring Servers): ftp://ring.aist.go.jp/archives/linux/knoppix/iso/knoppix_v5.3.1DVD_20080326_xen3.2.1-20080827.iso
- HTTP (Ring Servers): http://ring.aist.go.jp/archives/linux/knoppix/iso/knoppix_v5.3.1DVD_20080326_xen3.2.1-20080827.iso
- Bittorrent: http://www.rcis.aist.go.jp/project/knoppix/download/knoppix_v5.3.1DVD_20080326_xen3.2.1-20080827.iso.torrent

Contents

1 Boot of VMKnoppix

VKKnoppix includes “GRUB-IMA” as the bootloader and keeps the log at TPM/BIOS-ACPI with Trusted Boot. The following figure shows the GRUB Menu.



Contents of GRUB Menu

Menu Items	Usage
KNOPPIX 5.3.1 (normal kernel)	Boot normal KNOPPIX(Linux 2.6.24)
KNOPPIX/Xen 3.2.1	Boot Xen3.2.1 + Linux 2.6.18
KNOPPIX 5.3.1 (normal kernel + ima)	Boot Linux2.6.24-IMA (Integrity Measurement Architecture) for Trusted Computing. The OpenPTS and Remote Attestation verify the integrity and vulnerability of the KNOPPIX.
BitVisor 0.3	Launch BitVisor on Intel VT mode and return GRUB
boot from hd	Boot an OS on Hard Disk
gPXE	Network Boot. PXE(TFTP) or HTTP.
TPM Checker	Check the function of TCG-BIOS.
InetBoot-netfs	Internet Boot from a ISO file (VMKnoppix) on a HTTP Server
InetBoot-HTTP-FUSE	Internet Boot with HTTP-FUSE VMKnoppix. GuestOS is Plan9,NetBSD
BuidRoot Shell	Launch a shell of BuildRoot which is used InetBoot

- Confirm the “eth0”. Please run the following command to get an IP address from DHCP.

  # pump –i eth0

  - If your PC includes IEEE1394 (for example: Intel Mac), please add “**nofirewire**” kernel option (at the second line of GRUB).

2 Usage of Virtual Machines

Explain the usage of each virtual machine.

2.1 Xen

Select “KNOPPIX/Xen 3.2” at GRUB Menu and boot.

2.1.1 Usage of DomainU/HVM-Domain

VMKnoppix includes easy commands to boot virtual machine.

- ✧ The following command runs “DomainU” with the image of VMKnoppix DVD.

  # knoppixU

- ✧ The following command runs “HVM Domain” with the image of VMKnoppix DVD. (It requires IntelVT or AMD-V CPU).

  # knoppixHVM

  The command boots VMKnoppix as default, but it accepts an option (***file://Absolute Directory of ISO file*** or ***http://URL of ISO file***) for 1CD/DVD OS.

  #knoppixHVM http://example.com/knoppix/*.iso**

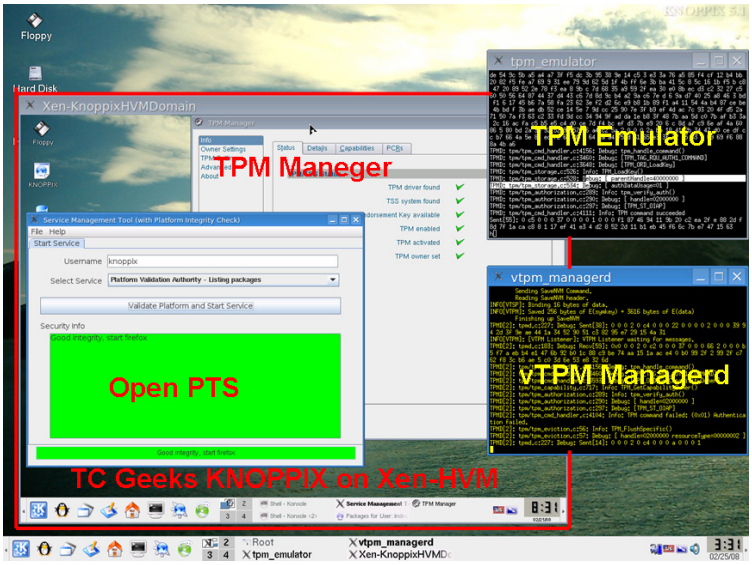
  #knoppixHVM file://home/knoppix/*.iso**

2.1.2 Usage of virtual TPM on Xen-HVM

Run the following command for virtual TPM(TPM Emulator) at first.

 # xen_vtpm start

2 windows (“tpm_emulator” and ”tpm_mangerd”) will appear. When there is only one window, kill the process with **xen_vtpm stop** and re-run **xen_vtpm start**.



After that the usage is same as the normal use. knoppixHVM and knoppixU has a TPM device. We recommend to use “**KNOPPIX for Trusted Computing Geeks**”to check the TPM on Xen-HVM. The usage is as follows.

#knoppixHVM http://example.com/knoppix/knoppix511-TC-Geeks-100.iso

#knoppixHVM file://tmp/knoppix511-TC-Geeks-100.iso

2.2 KVM, KQEMU, QEMU

Select "KNOPPIX 5.3.1 (normal kernel)" at GRUB Menu and boot. The following command automatically detects and inserts the suitable module for kvm, kqemu and qemu, in the order. KVM, KQEMU, and QEMU boot with the image of VMKnoppix DVD.

 # qemu-knoppix.sh

Option "**-no-kvm**" to cancel the KVM kernel module.

"**-no-kqemu**" to cancel the KQEMU kernel module.

"**-no-module**" to cancel the KVM/KQEMU kernel modules.

"**-tpm**" to enable a virtual TPM.

The command accepts ISO file with the following manner.

 # qemu-knoppix.sh http://example.com/knoppix/knoppix.iso

 # qemu-knoppix.sh file://tmp/knoppix.iso

Caution:

Please add "**nolapic**" option at GRUB when you boot on KVM.

2.2.1 Usage virtual TPM of KVM/QMEU

"qemu-knoppix.sh" script enables a virtual TPM with "-tpm" option.

 # qemu-knoppix.sh -tpm

It boots the image of VMKnoppix.VMKnoppix. Please select "KNOPPIX 5.3.1 (normal kernel + ima)" at GRUB Menu to try a trusted computing.

If you want to use Normal KVM command, run "**tpmd**" command before it. It set up a virtual TPM.

 # tpmd clear

 # kvm -m 512 -no-kvm-irqchip -L /usr/share/tcgbios -cdrom /dev/cdrom

When you use a CPU without Intel-VT/ADM-V or dis-enable the driver of KMV, you can use a virtual TPM. At that time, "kvm" command boots a QEMU.

 # rmmod kvm

 # rmmod kvm-intel

 # tpmd clear

 # kvm -m 512 -no-kvm-irqchip -L /usr/share/tcgbios -cdrom /dev/cdrom

2.2.2 Summary of Virtual TPM

Following table summarize the function of virtual TPM. The red character indicates the weak point.

	Xen-HVM	KVM	QEMU(Boot from KVM)
Host OS	Dom0 kernel is Linux2.6.18. It does not support least device drivers.	Latest Linux kernel. The drivers are better.	Latest Linux kernel. The drivers are better.
C P U	Intel VT or AMD-V is required	Intel VT or AMD-V is required.	Any x86 CPU.
Performance	Fast	Fast	Slow

I talk about the current status of Virtual TPM at “Virtualization Mini Summit at Ottawa Linux Symposium 2008”. Please refer the slide.

Virtual TPM on Xen/KVM for Trusted Computing
Kuniyasu Suzaki, Toshiki Yagi, Kengo Iijima, Nguyen Anh Quynh
http://virtminisummit.linux.hp.com/program/OLS08-Virtualization-Suzaki.pdf

2.2.3 Usage of QEMU x86_64 (AMD-V)

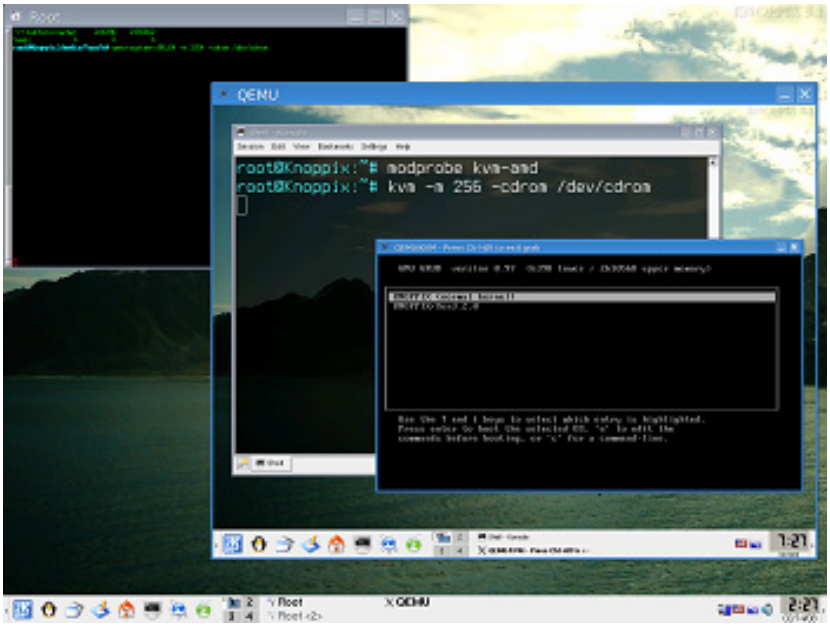
QEMU x86_64 emulates AMD-V Instruction Set and runs KVM on it. Unfortunately Xen can’t work well.

 # qemu-system-x86_64 -m 512 -cdrom /dev/cdrom

On the virtual machine KVM launches a virtual machine with AMD-V Instruction.

 # kvm -m 512 -cdrom /dev/cdrom

Select normal kernel and add “**nolapic**” kernel option at GRUB Menu.



2.3 VirtualBox

Select “KNOPPIX 5.3.1 (normal kernel)” at GRUB Menu and boot. Following commands set up VirtualBox.

 # modprobe vboxdrv
 # virtualbox

2.4 UML (UserMode Linux)

Select “KNOPPIX 5.3.1 (normal kernel)” at GRUB Menu and boot. Following command boots KNOPPIX on UML with VNC.

 # umlknx.sh

2.5 BitVisor 0.3

BitVisor is a secure virtual machine monitor running on Intel VT. It is developed for increasing security of OS which is used on Japanese Government. Current BitVisor0.2 is core only and has no special function. However we can get the drift with the easy installation.

2.5.1 Boot of BitVisor

Select “BitVosr” at GRUB Menu. BitVisor is launched on “root mode” of IntelVT and it returns to GRUB Menu. After that we can select any OS from the GRUB Menu. The OS is booted on “non-root mode” of IntelVT.

The OS installed on a hard disk is booted from the GRUB Menu “bootfrom hd0”. As default, the OS install the First partition is booted. If a OS is installed on the other partition, change the GRUB options “rootnoverify hd(0,0)”. The second value indicates the partition number. “hd(0,1)” means the booting from second partition. If Windows is installed on the hard disk, Windows boots on BitVisor.

When GRUB Menu “KNOPPIX5.3.1” is selected, KNOPPIX boots on BitVisor. Xen can NOT boot because BitVisor is installed on “root mode” of Intel VT.

BitVisor can works with “gPXE” for network boot.

2.5.2 Check the running of BitVisor

BitVisor shows the message ”F12 Pressed” on the SERIAL CONSOLE when F12 key is pressed. The function is not confirmed on Windows or X Window.

VMKnoppix includes GRUB-IMA for Trusted Boot. It keeps the boot log at TPM and BIOS-ACPI. The log is confirmed on KNOPPIX(Linux 2.6.25) by inserting TPM module. The log shows the SHA1 digest value of BitVisor.

 # sha1sum /cdrom/boot/isolinux/bitvisor.elf

aa28a31eeda42585813dd3d6f7be3fd117b69fcf /cdrom/boot/isolinux/bitvisor.elf

 # modprobe tpm_tis

 # mount –t securityfs none /sys/kernel/security

 # cat /sys/kernel/security/tpm0/ascii_runtime_mesurements

4 89f0284e00992d067654818a9f2c09bbaa31acde 05 [Booting CD ROM, - MATSHITADVD-RAM UJ-833S]

4 19d1733e8f9645c090f8fcce58a7f943a30fbc66 0d [IPL]

4 ec2afa621c866fd0c128d309e2415a4f49262acb 0d [IPL]

4 2cedbf54913d69d027c5b97e02763f921b16e345 06 []

4 8cdc27ec545eda33fbba1e8b8dae4da5c7206972 04 [Grub Event Separator]

5 8cdc27ec545eda33fbba1e8b8dae4da5c7206972 04 [Grub Event Separator]

5 bc74830d55c1cff5603df9ff93387b51d5db9f68 0e [IPL Partition Data]

5 d63d12ced978aca120bfe6ee7683e394c2ffaef0 05 [Boot Sequance User Intervention]

5 371436a31b138be9f75b887f02b9bd723cc21e4c 1105 []

8 **aa28a31eeda42585813dd3d6f7be3fd117b69fcf** 1205 [] **/*** BitVisor ***/**

5 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]

8 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]

8 be25adb01778393bbcae98ee871528fabfc85902 1005 []

4 ec2afa621c866fd0c128d309e2415a4f49262acb 0d [IPL]

4 2cedbf54913d69d027c5b97e02763f921b16e345 06 []

4 8cdc27ec545eda33fbba1e8b8dae4da5c7206972 04 [Grub Event Separator]

5 8cdc27ec545eda33fbba1e8b8dae4da5c7206972 04 [Grub Event Separator]

5 bc74830d55c1cff5603df9ff93387b51d5db9f68 0e [IPL Partition Data]

5 646b02b443f710cfb55debe234070588978828e5 1105 []

8 3efcce6615807a884992b9555f0a311fb8b474a6 1205 []

8 5c6e6c260a2d674fa13f5115b7eaf5499733e3f9 1405 []

5 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]

8 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]

8 fac33a1fc0ad42c07d00322d64c23f67567f334a 1005 []

3 Network Boot

VMKnoppix include 3 types of Network Boot: InetBoot, gPXE, OSCirclar.

3.1 InetBoot

InetBoot (GRUB + BuildRoot + HTTP-FUSE) is a **bootloader** which gets hypervisor, kernel and miniroot via Internet and reboots them with **"kexec"(Warm Reboot)**. InetBoot is consisted of a small Linux environment "BuildRoot". It setup network, download a kernel from a HTTP server, and reboot it with "kexec". Namely it works as a **PreBoot** environment. The GRUB Menu includes item "BuidRoot Shell" to run Shell of BuildRoot.

There are 2 ways to get disk image; **NetFS** and **HTTP-FUSE**. NetFS uses "httpfs" to mount a ISO file on a HTTP Server. HTTP-FUSE uses an Internet Virtual Disk "HTTP-FUSE CLOOP".

VMKnoppix includes some GRUB Menu items for InetBoot. It deeply depends on Network Interface.

3.2 gPXE

gPXE is an open source Network Bootloader. It works PXE boot as default. gPXE can boot from HTTP and iSCSI with some commands.

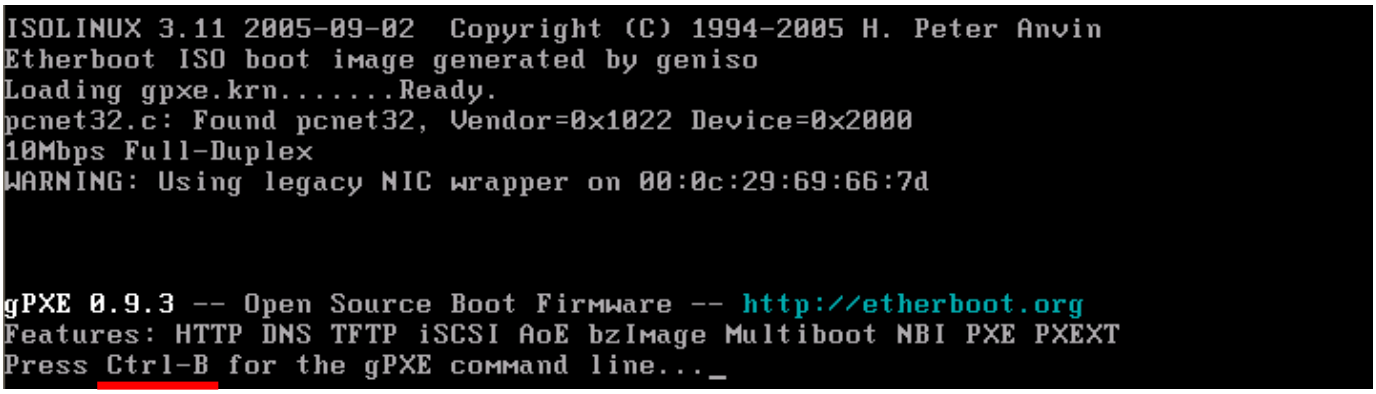
3.2.1 Boot of HTTP-FUSE KNOPPIX with gPXE

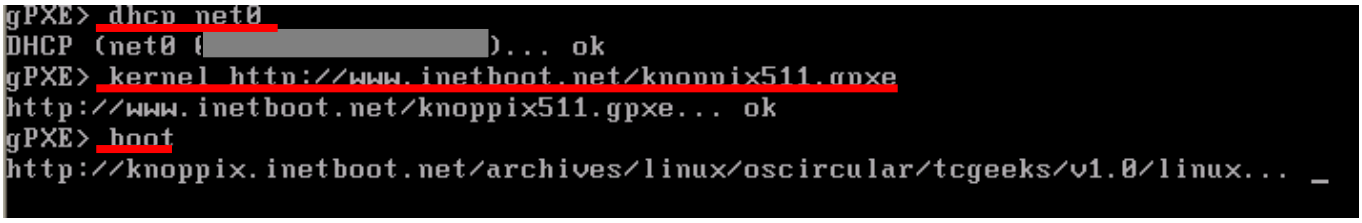
Select "gPXE" at GRUB Menu. gPXE tries PXE boot automatically. Before change the mode, press **CTL+B** and mode to shell mode. Execute the following commands on the shell to boot HTTP-FUSE KNOPPIX.

```
gPXE> dhcp net0
gPXE> kernel http://www.inetboot.net/knoppix511.gpxe
gPXE> boot
```

The first command sets up IP address with DHCP. It depends on network interface. If network interface is not recognized, network boot is not available.

The second command downloads a script to boot HTTP-FUSE KNOPPIX. The last command boots an OS with the downloaded kernel.





The upper example boots “KNOPPIX5.1.1”. If the second URL is changed with the following, KNOPPIX 5.0.1 or 4.0.2 will boot.

http://www.inetboot.net/knoppix501.gpxe

http://www.inetboot.net/knoppix402.gpxe

3.2.2 Combination of BitVisor and gPXE

gPXE is available after BitVisor is loaded. gPXE and booted OS is running on “non-root” mode of Intel VT.

3.3 OS Circular

OS Circular is a framework of Internet Disk Image Distributor for Virtual Machine.

3.3.1 On the normal kernel

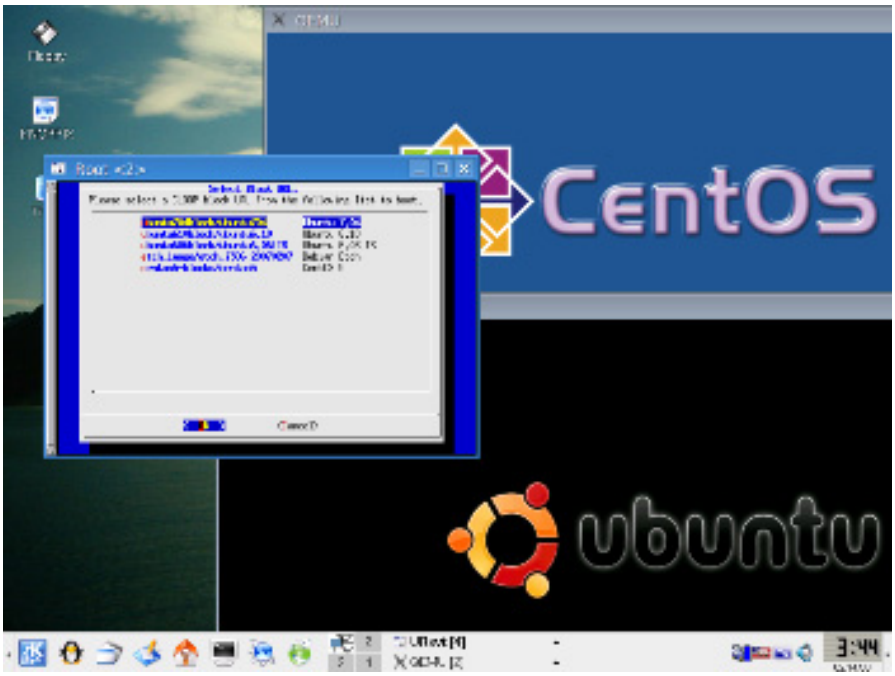
KVM/KQEMU/QEMU boots an OS with Internet Virtual Disk (Trusted HTTP-FUSE CLOOP). The following commands are used to boot an OS

#httpfuse-kvm

#httpfuse-kqemu

#httpfuse-qemu

Selection Menu of OS will appear. Select a desired one. When you are required to login, **“Account/Password” is “http-fuse/http-fuse”**.



3.3.2 On the Xen3.2.1

Xen-HVM can use Internet Virtual Disk (Trusted HTTP-FUSE CLOOP).

Setup the network and Xen at first.

 # pump –i eth0

 # /etc/init.d/xend start

The following command runs Xen-HVM with Internet Virtual Disk (Trusted HTTP-FUSE CLOOP).

#httpfuse-hvm

Selection Menu of OS will appear. Select a desired one. When you are required to login, **"Account/Password" is "http-fuse/http-fuse".**

3.3.3 Mount Internet Virtual Disk (Trusted HTTP-FUSE CLOOP)

Setup up mount points for Internet Virtual disk.

 # mkdir /var/tmp/blocks

The following mount points can use any name.

 # mkdir /media/thfc

 # mkdir /media/guestos

A "Mapping Table" file is downloaded from the following URL.

http://vmimage.inetboot.net/archives/linux/oscircular/pc/centos5-blocks/centos5.idx

http://vmimage.inetboot.net/archives/linux/oscircular/pc/etch_image/etch_i386-20070207.idx

http://vmimage.inetboot.net/archives/linux/oscircular/pc/etch_image/etch_i386-20061221.idx

http://vmimage.inetboot.net/archives/linux/oscircular/pc/ubuntu606block/ubuntu6.06LTS.idx

http://vmimage.inetboot.net/archives/linux/oscircular/pc/ubuntu610block/ubuntu6.10.idx

http://vmimage.inetboot.net/archives/linux/oscircular/pc/ubuntu704block/ubuntu704.idx

The flowing commands are an example to mount the root file system of CentOS5.

 # cd /var/tmp/blocks/

 # wget http://vmimage.inetboot.net/archives/linux/oscircular/pc/centos5-blocks/centos5.idx

 # httpstoraged -f

/media/htfs http://vmimage.inetboot.net/archives/linux/oscircular/pc/centos5-blocks/centos5.idx

A virtual disk file "/media/thfc/centos5" will appear.

The virtual disk use LVM. Run the following commands.

 # losetup /dev/loop0 /mountpoint/centos5

 # kpartx -a /dev/loop0

After that "loop0p1", "loop0p2" will appear under "/dev/mapper/". loop0p2 is a LVM partition.

 # lvmdiskscan

 # vgchange -a y

A device node /dev/VolGroup00/LogVol00 will be created. Mount the device and find the root file system of CentOS5.

#mount /dev/VolGroup00/LogVol00 /media/guestos

3.3.4 Load Balancing of Internet Virtual Disk (Trusted HTTP-FUSE CLOOP)

Trusted HTTP-FUSE CLOOP re-constructs a virtual disk with small block files. The block files are downloaded from HTTP servers. It is weak for network latency and the access speed become low when the network latency is long. To solve the network latency we deploy the servers worldwide. Current implementation offers 3 sites in US, 3 sites in Europe, and some sites offered by RING-Project in Japan. The nearest site is suggested by the DNS-Balance. If you are interesting in the load-balancing, check your download and the reference paper.

4 Trusted Computing (called "KNOPPIX for Trusted Computing Geeks")

The VMKnoppix includes the function of Trusted Computing, which is called "KNOPPIX for Trusted Computing Geeks". The Open Platform Trusted Services validates the **integrity of platform** and **vulnerability of applications** on VMKnoppix by the remote attestation which is a kind of Trusted Third Party. The information if vulnerability is based on DSA(Debian Security Advisory http://www.debian.org/security/) and CVE(Common Vulnerabilities and Exposures http://cve.mitre.org/).

The trusted computing runs on a TPM and a virtual TPM which is provided by Xen-HVM and KVM/QEMU.

4.1 Included Software

- GRUB-IMA1.1.0.0
  - http://trousers.sourceforge.net/grub.html
- kernel 2.6.24+IMA(Integrity Measurement Architecture)
  - http://sourceforge.net/projects/linux-ima
- Trousers0.3.1
  - http://trousers.sourceforge.net/
- TPM_Manager0.5
  - http://sourceforge.net/projects/tpmmanager
- OpenPTS v0.1.2 (Platform Trusted Services)
  - http://sourceforge.jp/projects/openpts/

4.2 Usage

The following method shows the usage of OpenPTS to validate the integrity of platform and vulnerability of applications. The original VMKnoppix includes vulnerable "iceweasel 2.0.0.12-1" and the validation is failed as default. You have to update the iceweasel to success the validation.

4.2.1 INVALID by Remote Attestation (Default Setting)

The following commands show the usage. In this case the username is "knoppix" but any name is OK.

 # mount -t securityfs none /sys/kernel/security/
 # tcsd
 # tpm_takeownership
Enter owner password: **knoppix**
Confirm password: **knoppix**
Enter SRK password: **(Just Return)**
Confirm password: **(Just Return)**

 # cp /opt/OpenPlatformTrustServices/tcdemo/dummy_system.data /var/lib/tpm/system.data
cp: overwrite `/var/lib/tpm/system.data'? **yes**
 # cd /opt/OpenPlatformTrustServices/tcdemo/
 # dmidecode > dmidecode

 # ../bin/pts-ca --propdir /opt/OpenPlatformTrustServices/tcdemo/

WARN [main] (?:?) - Known proplem on Thinkpad T60 and X60, FSM Trans was Failed, PUSH PUSH rc=1

ERROR [main] (?:?) - IBM BootImage of Knoppix511trust

ERROR [main] (?:?) - ConcurrentModificationException happen with GCJ. try to use adoptNode instead of import Node

Enter user's password:**knoppix**

 # ../bin/pts-cu --propdir /opt/OpenPlatformTrustServices/tcdemo/

Enter user's password:**knoppix**

WARN [main] (?:?) - Quoted but no FSM for PCR 8

WARN [main] (?:?) - Quoted but no FSM for PCR 10

WARN [main] (?:?) - Quoted but no Events for PCR 0, len=0

WARN [main] (?:?) - Quoted but no Events for PCR 2, len=0

ERROR [main] (?:?) - BootImage did not match Y5rFzfilzzJFl1kyxqQhVFCnuY8=

WARN [main] (?:?) - IMA Aggrigate validation was Failed - TODO Use PCR in IR

WARN [main] (?:?) - buf bcbe389ac4836462aee11301ac6395c84b623c200000000000000000000000000000000000003a3f780f11a4b49969fcaa80cd6e3957c33b22750000000000000000000000000000000000000075decad5939883814adb73adca947cdd781d4c63f95bd8e09c19d36d36a5fb4c0a5be9137ea737b00000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000

WARN [main] (?:?) - digest 104c129021038f96d4ad09d235cb9ec11c8b1f23

WARN [main] (?:?) - digest 4cd12acfecb05232c91831ae8e1d79d043d500ce

ERROR [main] (?:?) - Wrong SIgnature but CONTINUE

VR result : INVALID

VR reason : iceweasel-2.0.0.12-1.i386,OVAL/DSA(DSA-1614), CVE(CVE-2008-2933 CVE-2008-2785), is vulnelable!!! but no update,1 vulnelable packages are found,PCR[10] measurement is invalid,

ERROR : validation was failed

REASON : iceweasel-2.0.0.12-1.i386,OVAL/DSA(DSA-1614), CVE(CVE-2008-2933 CVE-2008-2785), is vulnelable!!! but no update,1 vulnelable packages are found,PCR[10] measurement is invalid,

4.2.2 VALID Case by Remote Attestation (when iceweasel is updated.)

The following commands show the usage. In this case the username is ”knoppix” but any name is OK.

 # apt-get update

 # apt-get install iceweasel

 # mount -t securityfs none /sys/kernel/security/

 # tcsd

 # tpm_takeownership

Enter owner password: **knoppix**

Confirm password: **knoppix**

Enter SRK password: **(Just Return)**

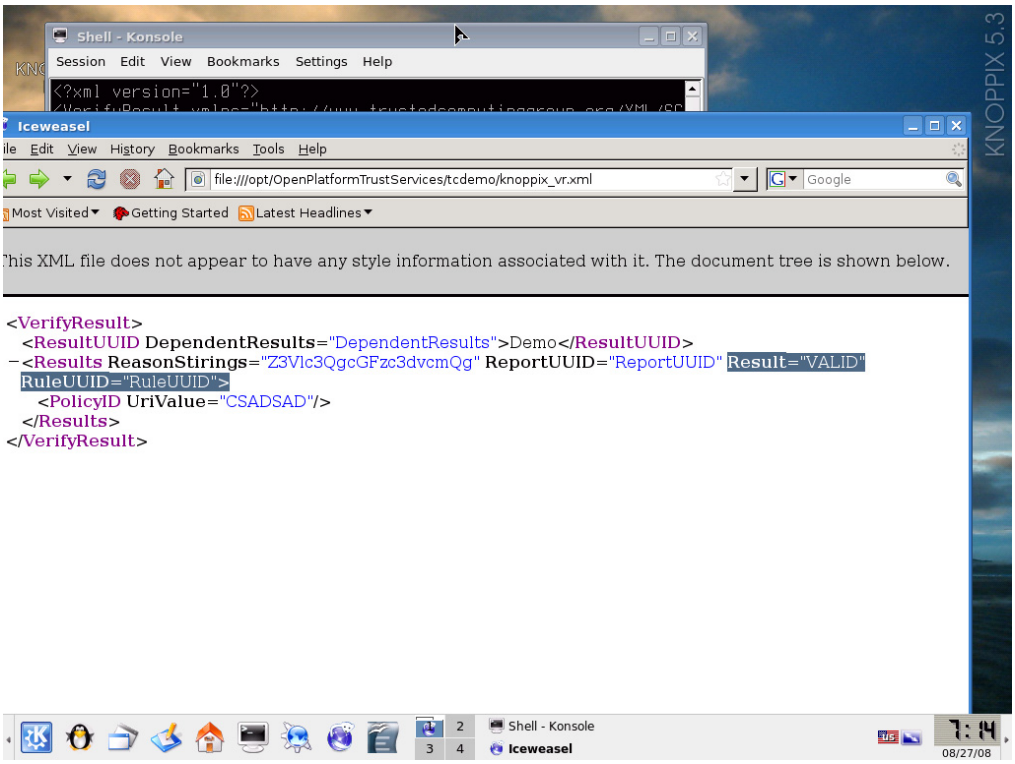
Confirm password: **(Just Return)**

```
# cp /opt/OpenPlatformTrustServices/tcdemo/dummy_system.data   /var/lib/tpm/system.data
cp: overwrite `/var/lib/tpm/system.data'? yes
# cd /opt/OpenPlatformTrustServices/tcdemo/
# dmidecode > dmidecode

# ../bin/pts-ca --propdir /opt/OpenPlatformTrustServices/tcdemo
 WARN [main] (?:?) - Known proplem on Thinkpad T60 and X60, FSM Trans was Failed, PUSH PUSH rc=1
ERROR [main] (?:?) - IBM BootImage of Knoppix511trust
Enter user's password:knoppix

# ../bin/pts-cu --propdir /opt/OpenPlatformTrustServices/tcdemo
Enter user's password:knoppix
 WARN [main] (?:?) - Quoted but no FSM for PCR 8
 WARN [main] (?:?) - Quoted but no FSM for PCR 10
 WARN [main] (?:?) - Quoted but no Events for PCR 0, len=0
 WARN [main] (?:?) - Quoted but no Events for PCR 2, len=0
ERROR [main] (?:?) - BootImage did not match Y5rFzfilzzJFl1kyxqQhVFCnuY8=
 WARN [main] (?:?) - IMA Aggrigate validation was Failed - TODO Use PCR in IR
 WARN [main] (?:?) - buf bcbe389ac4836462aee11301ac6395c84b623c2000000000000000000000000000000000000000003a3f780f11a4b49969fcaa80cd6e3957c33b2275000000000000000000000000000000000000000075decad5939883814adb73adca947cdd781d4c69516f1eb472d7c363d664b82a4e90fe2d0fb473d000000000000000000000000000000000000000000000000000000000000000000000000000
 WARN [main] (?:?) - digest 15fe00bb00ab2d7e0b0978174a5446c7c1fb3e56
 WARN [main] (?:?) - digest 34eafd4bad3b6563233ca45c3d258fe40c13fabe
ERROR [main] (?:?) - Wrong SIgnature but CONTINUE
```

The resut is returned to "/opt/OpenPlatfromTrustServices/tcdemo/knoppix_vr.xml". The file shows Resut="VALID" (following figure).



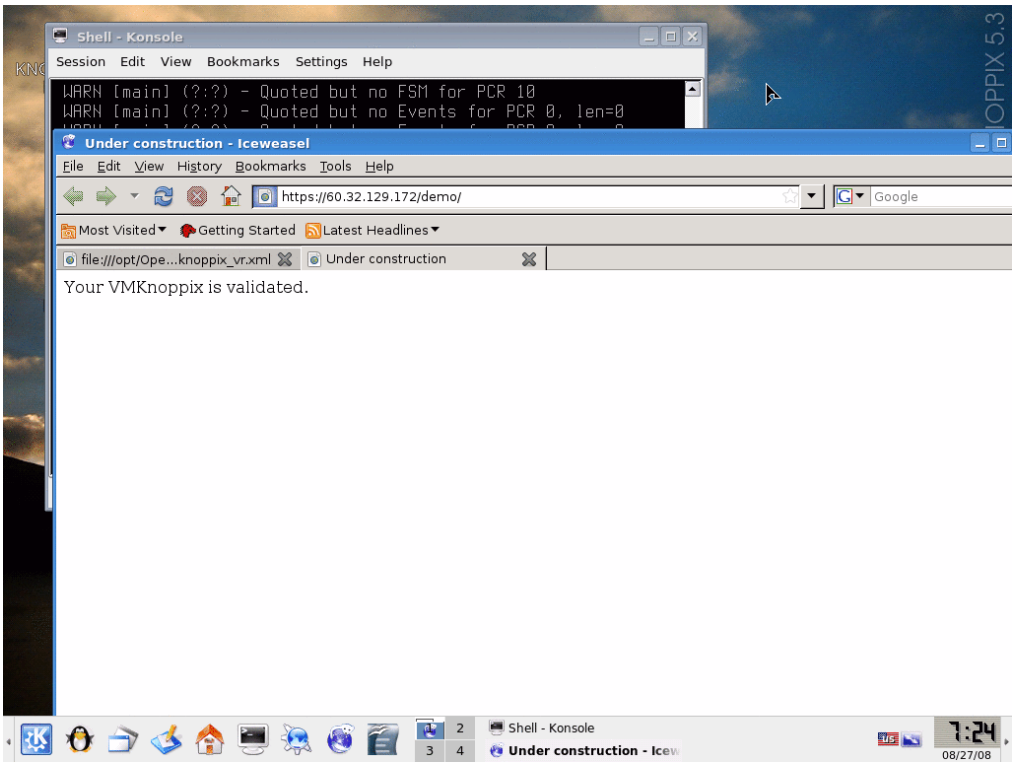
A browser “iceweasel” will be opened. The Secure Connection will be failed at the current setting. Please allow the following setting to show the home page.

Add Security Exception

https://60.32.129.172/demo Get Certificate

Confirm Security Exception

You will find the message ”Your VMKnoppix is validated.” (following figure).



The detail of command of OpenPTS is described at the following home page.

Command Reference of OpenPlatform Services

http://sourceforge.jp/projects/openpts/wiki/TcdemoCommandReference

Reference

[1] Kuniyasu Suzaki, Kengo Iijima, Toshiki Yagi, and Nguyen Anh Quynh, Trusted Boot and Platform Trust Services on 1CD Linux, IEEE International Forum on Trusted Infrastructure Technologies and 3rd Asia-Pacific Trusted Infrastructure Technologies Conference (APTC 2008)

[2] Seiji Munetoh, Megumi Nakamura, Sachiko Yoshihama, and Michiharu Kudo, "Integrity Management Infrastructure for Trusted Computing", IEICE TRANSACTIONS on Information and Systems, Vol. E91-D No. 5 pp. 1242-1251 (2008).

Abstract: http://search.ieice.org/bin/summary.php?id=e91-d_5_1242&category=D&year=2008&lang=E&abst=

Paper: http://search.ieice.org/bin/pdf.php?lang=E&year=2008&fname=e91-d_5_1242&abst=

5 Compilers

5.1 FailSafe-C

Fail-Safe C is a memory-safe implementation of the full ANSI C language. More precisely, it detects and disallows all unsafe operations, yet conforming to the full ANSI C standard (including casts and unions) and even supporting many "dirty tricks" common in many existing programs which do not strictly conform to the standard. This work also proposes several techniques---both compile-time and runtime---to reduce the overhead of runtime checks. By using the Fail-Safe C compiler, programmers can easily make their programs safe without performing heavy rewriting or porting of their code.

The following commands show a simple compilation and run. Please refer the original home page (https://staff.aist.go.jp/y.oiwa/FailSafeC/) for the detail.

$ fscc test.c –o test

$ ./test

5.2 VX32

VX32 is a user level sandbox that wishes to create secure, isolated execution environments in which to run untrusted extensions

The following commands show a simple compilation and run. Please refer the original home page (http://pdos.csail.mit.edu/~baford/vm/) for the detail.

$ vx32-gcc test.c -o test

$ vxrun ./test

(CAUTION: “test” is not executable.)

Paper: Bryan Ford and Russ Cox, “Vx32: Lightweight User-level Sandboxing on the x86”, USENIX Annual Tech 2008. pp293–306

http://www.usenix.org/events/usenix08/tech/full_papers/ford/ford.pdf

5.3 LLVM (Low Level Virtual Machine)

LLVM (Low Level Virtual Machine) is a compiler infrastructure, which is designed for compile-time, link-time, run-time, and "idle-time" optimization of programs. LLVM has an original byte-code and optimize it at run time. LLVM is used in the OpenGL pipeline of Mac OS X 10.5 (Leopard) to provide support for missing hardware features.

The following commands show a simple compilation and run. Please refer the original home page (http://llvm.org/) for the detail.

$ llvm-gcc –emit-llmv –c test.c –o test.bc

$ lli test.bc

(CAUTION: “test.bc” is a LLVM byte-code and lli execute it.)

6 Reference Paper/Presentation

[1] USENIX LISA 2007 (21st Large Installation System Administration conference) Dallas, USA, Nov. 14-17 "OS Circular: Internet Client for Reference", Kuniyasu Suzaki, Toshiki Yagi, Kengo Iijima, and Nguyen Anh Quynh
Paper http://www.usenix.org/events/lisa07/tech/suzaki.html
Silde PDF http://openlab.ring.gr.jp/oscircular/LISA07-Slide-suzaki.pdf

[2] ASPLOS 08 (Thirteenth International Conference on Architectural Support for Programming Languages and Operating Systems) Poster "TPM + Internet Virtual Disk + Platform Trust Services = Internet Client", Kuniyasu Suzaki, Kengo Iijima, Toshiki Yagi, Nguyen Anh Quynh, Megumi Nakamura and Seiji Muhetoh
Poster http://openlab.ring.gr.jp/oscircular/ASPLOS08-poster-slide.pdf
Leaflet http://openlab.ring.gr.jp/oscircular/ASPLOS08-poster-leaflet.pdf

[3] USENIX Annual Tech 2008 Poster "InetBoot and VMSeed; Trusted Internet Bootloader for Hypervisor and Guest OS", Kuniyasu Suzaki, Kengo Iijima, Toshiki Yagi, and Nguyen Anh Quynh
Poster http://openlab.jp/oscircular/USENIX08Poster-suzaki.pdf

[4] Linux Symposium 2008, BOF "OS Circular", Kuniyasu Suzaki
HP: http://www.linuxsymposium.org/2008/view_abstract.php?content_key=231

[5] Virtualization Mini Summit at Ottwa Linux Symposium 2008, Virtual TPM on Xen/KVM for Trusted Computing, Kuniyasu Suzaki, Toshiki Yagi, Kengo Iijima, Nguyen Anh Quynh
Slide: http://virtminisummit.linux.hp.com/program/OLS08-Virtualization-Suzaki.pdf

[6] IEEE International Forum on Trusted Infrastructure Technologies and 3rd Asia-Pacific Trusted Infrastructure Technologies Conference (APTC 2008), Trusted Boot and Platform Trust Services on 1CD Linux, Kuniyasu Suzaki, Kengo Iijima, Toshiki Yagi, and Nguyen Anh Quynh