

VMKnoppix 20080519 Version (based on KNOPPIX5.3.1 CD size)

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

<http://www.reis.aist.go.jp/project/knoppix/vmknoppix/index-en.html>

■ Special Features

- The based **KNOPPIX is updated to 5.3.1(kernel 2.6.24)**.
- Include secure virtual machine monitor "**BitVisor 0.2**".
- Update Xen to version 3.2.1.
- 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 "**GRUB-IMA(Integrity Measurement Architecture)**" which treats Trusted Boot.
- **Set up Xen3.2.1 + vTPM (TPM Emulator) for Trusted Computing**.
 - The virtual machine includes a TPM and TCG-BIOS and runs "KNOPPIX for Trusted Computing Geeks(Trusted Boot+Remote Attestation) on it.
- 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".
- Include QEMU091(x86_64) which offers ADM-V instruction set for virtual machine.
 - KVM runs on it but Xen-HVM doesn't.

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/>
- BitVisor <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>

Download

- File Name: knoppix_v5.3.1CD_20080326_xen3.2.1-20080519.iso
- MD5: 20b6114496fef6dde61e7ed6fcf82c09
- FTP: (Ring Servers): ftp://www.ring.gr.jp/archives/linux/knoppix/iso/knoppix_v5.3.1CD_20080326_xen3.2.1-20080519.iso
- HTTP (Ring Servers): http://www.ring.gr.jp/archives/linux/knoppix/iso/knoppix_v5.3.1CD_20080326_xen3.2.1-20080519.iso

- Bittorrent: http://www.rois.jp/project/knoppix/knoppix_v5.3.1CD_20080326_xen3.2.1-20080519.iso.torrent

Contents

1	Boot of VMKnoppix.....	3
2	Usage of Virtual Machines.....	3
2.1	BitVisor 0.2.....	3
2.1.1	Boot of BitVisor.....	4
2.1.2	Check the running of BitVisor.....	4
2.2	Xen.....	5
2.2.1	Usage of DomainU/HVM-Domain.....	5
2.2.2	Usage of vTPM on Xen-HVM.....	5
2.3	KVM/KQEMU/QEMU.....	6
2.3.1	Usage of QEMU x86_64 (AMD-V).....	6
2.4	VirtualBox.....	6
2.5	UML (UserMode Linux).....	7
3	Network Boot.....	7
3.1	InetBoot.....	7
3.2	gPXE.....	7
3.2.1	Boot of HTTP-FUSE KNOPPIX with gPXE.....	7
3.2.2	Combination of BitVisor and gPXE.....	8
3.3	OS Circular.....	8
3.3.1	On the normal kernel.....	8
3.3.2	On the Xen3.2.1.....	9
3.3.3	Mount Internet Virtual Disk (Trusted HTTP-FUSE CLOOP).....	9
3.3.4	Load Balancing of Internet Virtual Disk (Trusted HTTP-FUSE CLOOP).....	10
4	Reference Paper/Presentation.....	10

1 Boot of VMKnoppix

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

```

GNU GRUB  version 0.97-ima-1.1.0.0 (638K lower
-----
KNOPPIX 5.3.1(normal kernel)
KNOPPIX/Xen3.2.1
BitVisor
boot from hd0
gPXE
InetBoot-netfs VMKnoppix(Xen3.2.0)
InetBoot-netfs VMKnoppix(Xen3.1.1)
InetBoot-netfs VMKnoppix(Xen3.1.0)
InetBoot-netfs VMKnoppix(Xen3.0.4.1) Oprofile
InetBoot-netfs VMKnoppix(Xen3.0.4.0)
InetBoot-HTTP-FUSE Xenoppix+Xen 2.0.6
InetBoot-HTTP-FUSE Plan9 (Xenoppix+Xen 2.0.6)

```

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
BitVisor	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.
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 chell of BuildRoot which is used InetBoot

- Confirm the “eth0”. Please run the following command to get an IP address form 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 BitVisor 0.2

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.

2.1.1 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 form 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 form 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.

2.1.2 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.

```
# modprobe tpm_tis
```

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

```
# cat sys/kernel/security/tpm0/ascii_runtime_measurements
```

```
4 7ca42b22324927c400263bae94e1e7cc28655532 05 [Booting CD ROM]
4 425d2011ed8849ef2fafd64bef72361b5eb8497f 0d [IPL]
4 b617e60559d6d53123021e33a7b18d9c51a56dd5 0d [IPL]
4 2cedbf54913d69d027c5b97e02763f921b16e345 06 []
4 8cdc27ec545eda33fbba1e8b8dae4da5c7206972 04 [Grub Event Separator]
5 8cdc27ec545eda33fbba1e8b8dae4da5c7206972 04 [Grub Event Separator]
5 0fd9f4e3a2b318a0d11645c0c388cb0b68680d67 0e [IPL Partition Data]
5 d63d12ced978aca120bfe6ee7683e394c2ffaef0 05 [Boot Sequence User Intervention]
5 371436a31b138be9f75b887f02b9bd723cc21e4c 1105 []
8 bcfe2fb3a02c2f35959239663003bede6db55a0f 1205 []      /** BitVisor **/
5 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]
8 2431ed60130faeaf3a045f21963f71cacd46a029 04 [OS Event Separator]
8 be25adb01778393bbcae98ee871528fabfc85902 1005 []
4 b617e60559d6d53123021e33a7b18d9c51a56dd5 0d [IPL]
4 2cedbf54913d69d027c5b97e02763f921b16e345 06 []
4 8cdc27ec545eda33fbba1e8b8dae4da5c7206972 04 [Grub Event Separator]
5 8cdc27ec545eda33fbba1e8b8dae4da5c7206972 04 [Grub Event Separator]
5 0fd9f4e3a2b318a0d11645c0c388cb0b68680d67 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 []
```

2.2 Xen

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

2.2.1 Usage of DomainU/HVM-Domain

VMKnoppix includes easy commands to boot virtual machine.

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

```
# knoppixU
```

- ✧ The following command runs “HVM Domain” with the image of VMKnoppix CD. (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 OS.

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

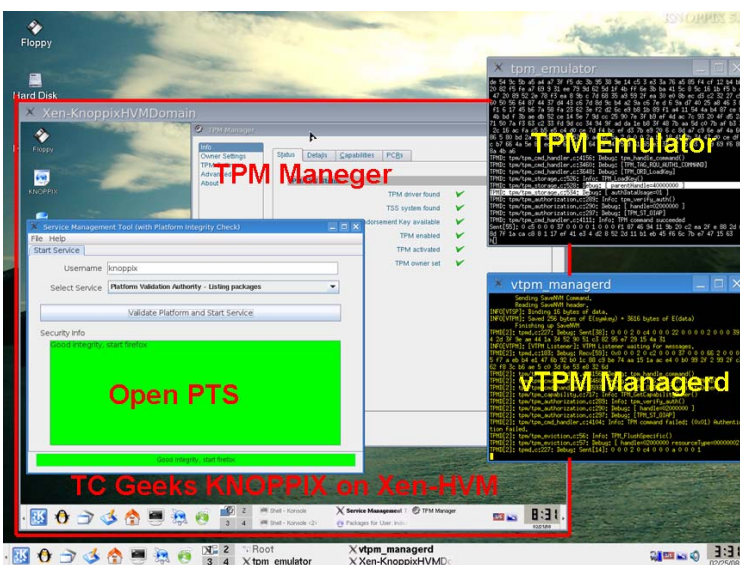
```
#knoppixHVM file://home/knoppix/***.iso
```

2.2.2 Usage of vTPM on Xen-HVM

Run the following command for vTPM(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
```

2.3 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/QEMU boot with the image of VMKnoppix CD.

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 a KVM/KQEMU kernel modules.

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.

2.3.1 Usage of QEMU x86_64 (AMD-V)

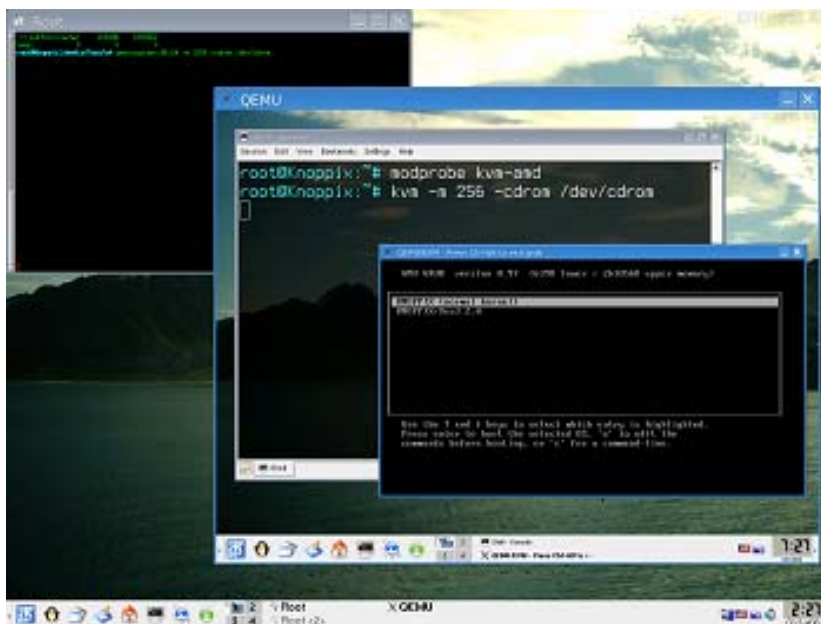
QEMU x86_64 emulates AMD-V Instruction Set and runs KVM on it. Unfortunately Xen can't work well.

```
# 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.



2.4 VirtualBox

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

```
# modprobe vboxdrv
```

```
# virtualbox
```

2.5 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
```

3 Network Boot

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

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 form 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 form 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.

```

ISOLINUX 3.11 2005-09-02 Copyright (C) 1994-2005 H. Peter Anvin
Etherboot ISO boot image generated by geniso
Loading gpxe.krn.....Ready.
pcnet32.c: Found pcnet32, Vendor=0x1022 Device=0x2000
10Mbps Full-Duplex
WARNING: Using legacy NIC wrapper on 00:0c:29:69:66:7d

gPXE 0.9.3 -- Open Source Boot Firmware -- http://etherboot.org
Features: HTTP DNS TFTP iSCSI AoE bzImage Multiboot NBI PXE PXEXT
Press Ctrl-B for the gPXE command line..._

```

```

gPXE> dhcp net0
DHCP (net0 {          })... ok
gPXE> kernel http://www.inetboot.net/knoppix511.gpxe
http://www.inetboot.net/knoppix511.gpxe... ok
gPXE> boot
http://knoppix.inetboot.net/archives/linux/oscircular/tcgeeks/v1.0/linux... _

```

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  
# httpstorged -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 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>
Slide 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
Pospter <http://openlab.ring.gr.jp/oscircular/ASPLOS08-poster-slide.pdf>
Leaflet <http://openlab.ring.gr.jp/oscircular/ASPLOS08-poster-leaflet.pdf>
- [3] Linux Symposium 2008, BOF “OS Circular”, Kuniyasu Suzaki
HP: http://www.linuxsymposium.org/2008/view_abstract.php?content_key=231