

# InetBoot and VMSeed: Trusted Internet Bootloader for Hypervisor and Guest OS

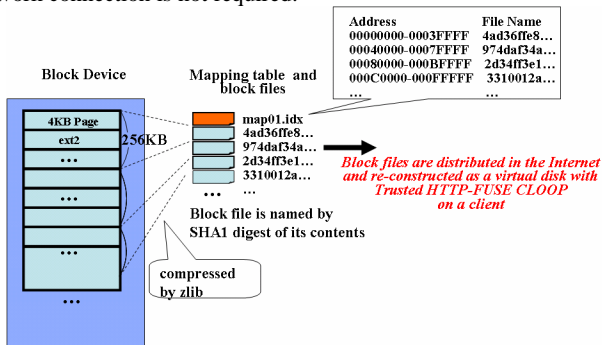
Kuniyasu Suzaki, Kengo Iijima, Toshiki Yagi, Nguyen Anh Quynh,  
National Institute of Advanced Industrial Science and Technology

## Hypothesis

- ◆ **Internet comes to be a BOOTABLE Device**
  - Hard Disk is a cache.
  - ✧ We developed “Trusted HTTP-FUSE CLOOP”.
  - Maintenance is a matter of OS supplier.
  - *We prepare bootloader only.*
  - ✧ We developed “InetBoot” and “VMSeed”.
- ◆ **Internet is dangerous.**
  - **PreBoot Verification** and **Trusted Computing** keep security.

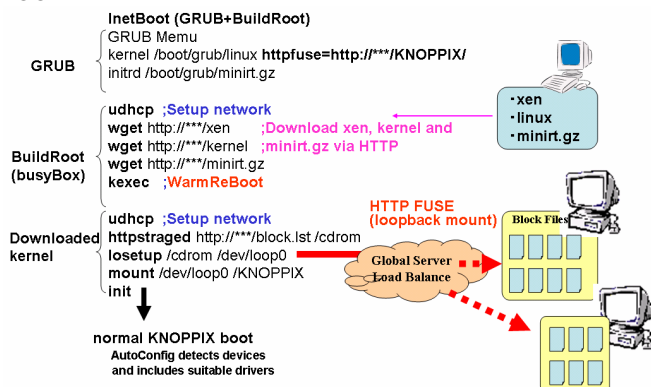
## Internet Block Archive: Trusted HTTP-FUSE-CLOOP

- ◆ A virtual block device is reconstructed by the block files downloaded via Internet.
- ◆ Each file has SHA1 file name and the driver has the mapping table.
- ◆ The contents are validated when it mapped to the block device.
- ◆ The block files are cached at local storage and reused. If fully cached, network connection is not required.



## InetBoot is a small Linux which works as a bootloader.

- ◆ It is consisted of GRUB and BuildRoot (BusyBox). (6MB)
- ◆ Download a hypervisor, kernel and miniroot, then reboot the machine with them using “kexec” system call of Linux.
- ◆ The root file system is obtained via Internet with Trusted HTTP-FUSE CLOOP



## VMSeed is an initial virtual disk image for a virtual machine.

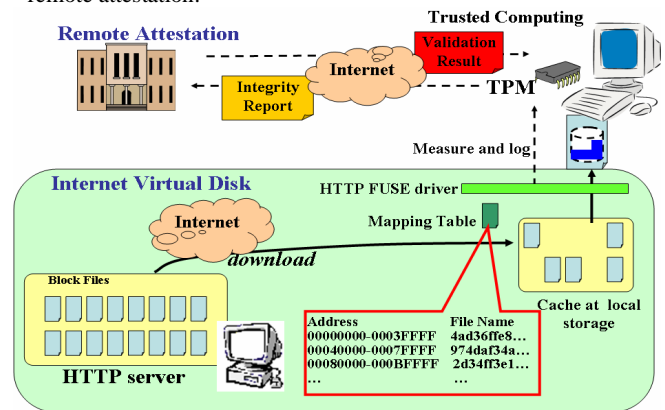
- ◆ The virtual disk file includes a kernel and miniroot only.
- ◆ The initial image is small because of **sparse virtual disk format** (e.g., “vmdk” of VMWare, “vdi” of VirtualBox, “hdd” of Parallels)
- ◆ The root file system is obtained via Internet. **The virtual disk grows as by use of the guest OS because the block files are cached.**

## PreBoot Verification

- ◆ InetBoot can include virus check tools in the BusyBox and verify the target OS before booting.
- ◆ InetBoot can include trusted computing.
  - Trusted Boot keeps the incident of boot procedure into the secure chip “TPM(Trusted Platform Module)”.
  - The incident is verified by the Remote Attestation.
  - We plan to integrate GRUB-IMA, Linux-IMA kernel (Integrity Measurement Architecture), TrouSerS, OpenPTS to InetBoot.

## Trusted Computing is applied to Client OS

- ◆ The client OS can include trusted boot and check the integrity by the remote attestation.



## Current Implementation

- ◆ InetBoot and VMSeed were released
  - InetBoot: <http://openlab.jp/oscircular/inetboot/>
    - ✧ Boot Xenopix (Xen2.0.6) with a Guest OS (Pan9 on Xen-DomU or NetBSD on Xen-DomU), and KNOPPIX (511, 501, 402)
  - VMSeed: <http://openlab.jp/oscircular/vmseed/>
    - ✧ For **VMWare, VirtualPC, VirtualBox, Parallels, Xen, KVM, QEMU**
    - ✧ Boot KNOPPIX (511, 501, 402).

## Related Work

VMSeed resembles to LivePC of Moka5 which uses streaming and caching of virtual disk images but VMSeed does not require any change of the virtual machine. VMSeed is contents of virtual disk file which utilize the sparse virtual disk format. VMSeed is applied to many virtual machines.

## Future Work

We will integrate Dynamic Root of Trust Measurement, which create trusted code execution, into InetBoot. It requires hardware supports (e.g. Intel TXT or AMD SVM). The technology enables trustworthy Warm Reboot using “kexec”.

## Reference

- [1] K.Suzaki,et.al., OS Circular: Internet Client for Reference, USENIX LISA 07.