“OS-Circular”: A Framework of Internet Client with Xen

http://openlab.jp/oscircular/

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

• Purpose of Internet Client
• What is OS Circular?
  – VM-Loader “Xenoppix”
  – Globalized Virtual Disk “HTTP-FUSE CLOOP”
    • Split & compressed & Trusted (Measured) Loopback device
    • Requirement of server is HTTP only.
  – Periodically security updated “Guest OS”
• Current Implementation & Future Work
  – Trusted Boot with TPM, Trusted Network Connect
  – Linkage of Vulnerability Database
• Conclusions
Purpose of OS Circular

- Framework of Internet client for anonymous users (OS Migration System).
  - Boot OS on anonymous PC without installation.
  - Deal with Disconnect network for mobile computing
    - Image of OS can be cached on local storage.
  - The OS is periodically updated.
    - But it allows to rollback to previous image.

- To be trusted service (discuss later)
Strategy of deployment

- **Policy**
  - Utilize popular/inexpensive Internet service and Client PC.
    - Most researches assume special service on the server. They prevent world wide deployment.
    - Current PC is cheap and powerful.

- **Client Centric System**
  - VM is running on a Client. OS Image is obtained via HTTP servers.
  - Reduce requirements for server and makes easy world wide scalability.
Related Work (OS Migration)

• **OS Zoo**
  - Distribute Virtual Disk files of QEMU for Linux, Minix, Plan9, OpenSolaris, etc.

• **FLOZ (Free Live OS Zoo)**
  - The GUI of QEMU is transferred by VNC to Web Browser on Client PC.
  - **Server Centric System**
    - Bad response because the server exits in Italy
    - Guest OS has no network service because of security & resource

• **Collective [HostOS’03][NSDI’05]**
  - Cache based System Management
    - Based on COW image of VMware
    - COW files are shared by NFS over SSH
## Comparison

<table>
<thead>
<tr>
<th>VM</th>
<th>Type of Management</th>
<th>Disk Image</th>
<th>Differential update</th>
<th>Transfer</th>
<th>Security on Transfer</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Circular</td>
<td>Xen (HVM)</td>
<td>Client Centric</td>
<td><strong>Trusted HTTP-FUSE CLOOP</strong></td>
<td>HTTP</td>
<td>Blocks are measured on Client</td>
</tr>
<tr>
<td>Collective</td>
<td>VMware</td>
<td>Client Centric</td>
<td>VMware disk file</td>
<td>COW of VMware</td>
<td>NFS over SSH</td>
</tr>
<tr>
<td>OS Zoo</td>
<td>QEMU</td>
<td>Client Centric</td>
<td>QEMU disk file</td>
<td>HTTP &amp; FTP</td>
<td>VNC</td>
</tr>
<tr>
<td>FLOZ</td>
<td>QEMU</td>
<td>Server Centric</td>
<td></td>
<td>VNC</td>
<td></td>
</tr>
</tbody>
</table>
OS Circular

- OS Circular is **Client Centric System** which utilizes virtualization technology.
  - “VM Loader” + “Globalized Virtual Disks”
  - Client PC boots with the VM Loader and get Guest-OS images via Globalized Virtual Disks
    - **Guest-OS images are updated periodically** on the server and they are executed on Client PC.
VM Loader

• VM Loader is consisted of “Virtual Machine software” and host OS which runs Virtual Machine

• Virtual Machine offers an Abstraction Layer which is a common PC environment on any PCs.
  – The abstraction is used for other researches of OS migration.
    • SoulPAD [Mobisys’05], VAT of Collective[NSDI’05], Internet Suspend/Resume[WMCSA’02] use VMware
    • Full Virtualization enables us to use normal installer and security management for Guest OS.

• The host OS supports real device drivers
  • KNOPPIX is used [SoulPAD,VAT of Collective], because KNOPPIX automatically detects available devices and loads the appropriate Linux drivers.
“Xenoppix” as VM Loader

- Xenoppix (2005.09～) = Xen + KNOPPIX(1CD Linux)
  - Old Xenoppix used Para-Virtualization(Xen2.0.6) and included Plan9 & NetBSD.
  - Current Xenoppix runs Para & Full Virtualization of Xen.
    - Xenoppix is renamed to VMKONPPIX.
    - KNOPPIX works on Domain0 of Xen (as host OS).
  - Xen has no device drivers and utilize the drivers of the OS on Domain0. “Autoconfig” of KNOPPIX detects devices and setup drives.
  - So, Xen and KNOPPIX is the best marriage.
Globalized Virtual Disk

- Virtual Disk is Block Level Abstraction.
- The requirement for OS Migration. (Pfaff[NSDI’06])
  - Versioning
    - Partial update & Rollback
  - Globalization
    - World Wilde Deployment
    - Network/Storage Transparent
      - Handle network (dis/re)-connection for mobile computing
  - Security
    - OS itself should maintained by Security Software
    - Virtual disks have to keep validness of contents

- We developed “Trusted HTTP FUSE CLOOP”.

Trusted HTTP-FUSE CLOOP (1/2)

- Original block device is split by 256KB and compressed by zlib. Each data is saved to each block file.
- Block files are managed by “index” file which includes location information.
  - “index” file works as a header of CLOOP.
- Block file name is a SHA1 value of its contents.
  - If there is a same contests blocks, they are held together a same name file and reduce total storage space.
  - The basic idea is resemble to “Venti of Plan9”[USENIX’02]
- Block files are reconstructed to a CLOOP file by FUSE wrapper.
  - FUSE is a User-land File System.
    - http://fuse.sf.net
- Each block file is measured with the SHA1 file name when it mapped to CLOOP.
Block Device

4KB Page
ext2
...
...
...
...
...
index and block files

index.idx
4ad36ffe8...
974daf34a...
2d34ff3e1...
3310012a...
...
...

The block files are reconstructed as a virtual disk with HTTP-FUSE CLOOP

compressed by zlib
Trusted HTTP-FUSE CLOOP (2/2)

- When a file is updated or created on an original block device, the relevant block files are newly created with new SHA1 name. The “index” file are also renewed.
  - Old block files are reusable.
- HTTP for file deliver
  - Most popular and well designed.
    - Web hosting is inexpensive for world wide deployment.
    - 80 port is usually opened.
      - Other network block devices use special port which is usually closed.
- Block files are network/storage transparent.
  - Block files are cached and reused on local storage.
  - If necessary block files are stored in a local storage, network connection is not necessary.
Block Device (2GB)

4KB Page
ext2
...
...
...

256KB

CLOOP file

Index.idx
4ad36ffe8...
974daf34a...
2d34ff3e1...
3310012a...
...

Same files
Reusable for FUSE

FUSE driver

apt-get install ...

Update
Each block file is measured with its file name at reading.

Contents SEVER block files

block files /tmp/blocks

CLOOP file(700MB) /cdrom/KNOPPIX

# losetup /dev/CLOOP /cdrom/KNOPPIX

CLOOP driver

Cache 64KB

decompress

FUSE driver

header (location data)

Obtain in security

Extract

4KB Page
ext2
Loopback(2GB)

Access
Two type of Security

• The OS image has to keep security
  – The OS is updated periodically by package manager.
    • “yum” of Fedora or “apt-get” of Debian
    • It should be Semi-automatic.
  – The target includes the kernel.
    • We have to use Full Virtualization.

• The way of distribution
  – Index file is obtained in secure way but the block files are downloadable from un-trusted servers.
  – The contents are measured on a Client.
  – We have to reboot Guest OS to updated OS image.
Partial Update

Security Update

Xen HVM

Index Files

New Index file

Block Files

New Block Files

Cache files at local storage

HTTP Server

Internet

On demand download

Client PC

Updated OS

Master PC

New Block Files

Xen HVM

Client PC
World Wide Deployment of Server

- We utilize inexpensive Web Hosting Service.
  - 5GB/ month from $10
DNS request
Resolve **select.inetboot.net** to shorten *latency*

- **Client**
- **Web server for HTTP-FUSE Xenoppix**
- **DNS server:** **ns.inetboot.net**
- **Block files**

**DNS-Balance**

ASK the nearest server for **select.inetboot.net**
XXX.168.0.10
YYY.10.0.19

**RADB** (Routing ASSET DATABASE)
Current Implementation of OS Circular

• VM Loader
  – Xenoppix (Xen 3.0.4 + KNOPPIX 5.1.1)
  – Debian package
    • Trusted HTTP-FUSE CLOOP
    • Setup script for OS Circular

• OS Images is obtained by Trusted HTTP-FUSE CLOOP
  – Debian GNU/Linux
    • Periodically updated with “apt-get” command
  – FreeBSD
Performance

- ThinkPAD T60 (Core Solo T1300 1.67Ghz)
  - Xen 3.0.4 HVM Domain
  - Debian GNU/Linux boot till GDM
To be Trust

• There are some problems
  A) Current Version has to trust Xenoppix.
      • Can’t prevent Virtual Machine Based Rootkit (Subvirt[SSP’06])
  B) Index file have to distribute in secure.
  C) There is no way to authenticate that vulnerable applications are replaced correctly on the updated OS.
Discussions (1/2)

• Trusted Boot with TPM (Trusted Platform Module)
  – The boot procedure is measured and the measurements are registered at PCR (Platform Configuration Register) of TPM.
  – The values of PCR are wrapped and reported to Remote Attestation

• Trusted Network Connect
  – Allow connection for the Client which is authenticated by Remote Attestation

• The values of PCR are used for authentication of Xenoppix. (A)
• The “index” file is obtained using Trusted Network Connect (B)
  – It enables to boot commercial OS on OS Circular.
Discussions(2/2)

• Linkage of Vulnerability Database
  – The update of Guest OS should be link to Vulnerability Databases.
  • CVE (Common Vulnerabilities and Exposures )
    – http://cve.mitre.org/

• We can check that the OS image doesn’t include vulnerable software. (C)
Conclusions

• OS Circular is Framework of Internet Client which is consisted of VM Loader “Xenoppix” and Global Virtual Disk “Trusted HTTP-FUSE CLOOP”.

• The current targets are Debian GNU/Linux and FreeBSD.
  – Debian is updated by “apt-get” semi-automatically.

• Future work
  – OS Circular will integrate Trusted Boot and guest OS will link to Vulnerability Database.
Related Presentation

• Linux Symposium 2006
  – “HTTP-FUSE Xenoppix”

• Linux Kongress 2006
  – “Trusted Boot of HTTP-FUSE KNOPPIX”
  – [http://www.linux-kongress.org/2006/abstracts.html#4_2_2](http://www.linux-kongress.org/2006/abstracts.html#4_2_2)

• Virtualization Miniconf at Linux.Conf.Au 2007
  – OS Circulation environment “Trusted HTTPFUSE Xenoppix”

• Embedded Linux Conference 2007
  – HTTP-FUSE PS3 Linux which is internet boot framework with kboot