# Hardening Enterprise Linux

## Securing your Linux distribution

Toshaan Bharvani - VanTosh bvba

<toshaan@vantosh.com>


GSE/IMUG 2014


25 March 2014

# $ whoami

Toshaan Bharvani @ VanTosh

- From Antwerp, Belgium
- Self-employed engineer/trainer (available for hire)
- Involved with Enterprise OS : `RHEL/CentOS`, `IBM AIX`, `SLES`, ...
- Likes to keep everything secure : `SELinux`, `WebSec`, ...
- Lives in a virtual world : `KVM`, `PowerVM`, `z/VM`, `Xen`, `LXC`, ...
- Likes automation : `Ansible`, `Puppet`, ...
- Works on both hardware and software side
- Wants to take over the world
- Twitter : @toshywoshy
- Blog : `http://www.toshaan.com`
- Company : `http://www.vantosh.com`

Hardware

Software

sVirt

Conclusion

The End

# Table of contents

1. Hardware
2. Software
3. sVirt
4. Conclusion

Hardware

Software

sVirt

Conclusion

The End

# 1

# Hardware

# Physical Hardware

- Set up a BIOS/UEFI/microcode/bootloader password
- Restrict booting to your boot device only
- Lock your machines to the rack
- Disable USB support on the server
- Disable VGA output
- Configure your management port and secure it
- Install your OS/software on an installation site

# Virtual Hardware

- CPU
  - Hyperthreading
  - Logical mapping
  - Pinning
- Memory
  - Dedicated
  - Ballooning
  - Backing pages
- Networking
  - Dedicated
  - Shared

# 2

# Software

# General

- Install only what you require on that system
  - Minimal bare install is about 218 packages
- Encrypt all data and trafic
  - Also the data going over “trusted” networks
  - Use end-to-end encryption
- Seperate and segregate functions
- Use different networks for isolation
- Grant the least priviliges required
- You do not need a graphical interface
- Disable all unnecessary services

# Disk

- Partition your disk
  - boot partition : /boot/
  - root partition : /
  - home partition : /home
  - log partition : /var/log
  - temp partition : /tmp
  - data partition : ...
- Make use of `nosuid`, `noexec`, `nodev` on partition that do no require this
- Use drive or file system encryption
- Protect GRUB
  - Password : password –encrypted <password>
  - Redirect to secure console

# Networking

- Enable only IP stack relevant to your network
- Make use of physical or virtual tagging
- Create VLAN enabled network devices
- Close all unnecessary ports : input and output
- (Rate)Limit your port for (ab)usage

# sysctl : networking

- Don't reply to broadcasts (DDoS)
- Protect from bad icmp error messages
- Protect againt SYN flood attack
- Log all suspicion packets : spoofed, source routed, and redirects
- Don't allow source routed packets
- Enable reverse path filtering
- Disable outside alterations to the the routing tables
- Disable forwarding an redirects (router)

# SSH protection

- Larger key lengths
- Run on a different port then 22
- Disable protocol 1
- Increase log level to display key login
- Short login grace time
- Disable root login over ssh
- Enable strict mode (make sure your permissions and labels are correct)
- Set a maximum authentification tries per login session
- Set a maximum number of session a user can login
- Enable public key authentication and disable password authentication
- Disable empty password login
- Only give certain users ssh access

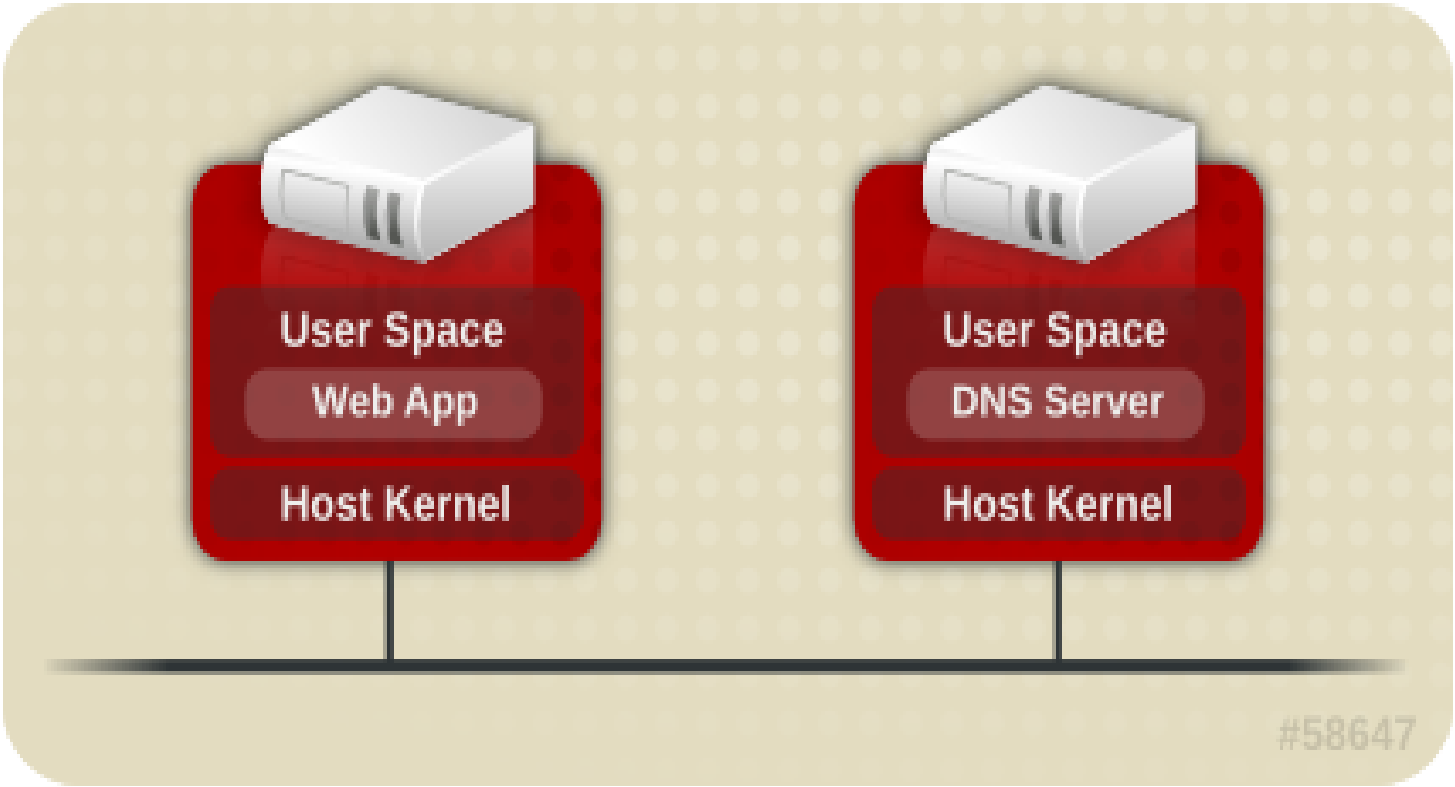
# Login access

- Do not allow changing the kernel bootup
- Secure access to runlevel 1
- Disable active consoles
- Disable the three finger salute
- Restrict root console login
- Disable unnecessary users
- Use sudo and logging to track your root access
- Only give sudo tty to users that really require it

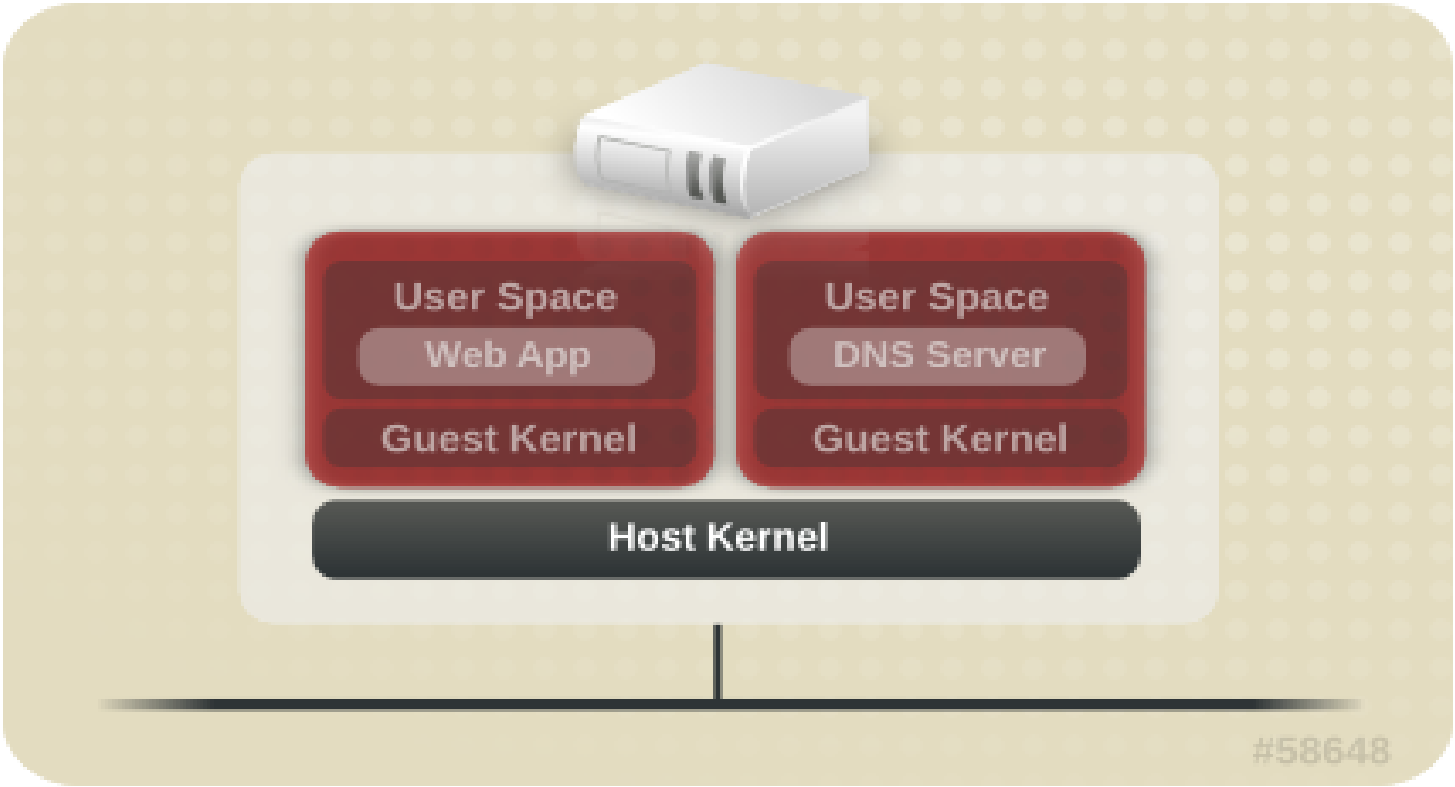
# 3

# sVirt

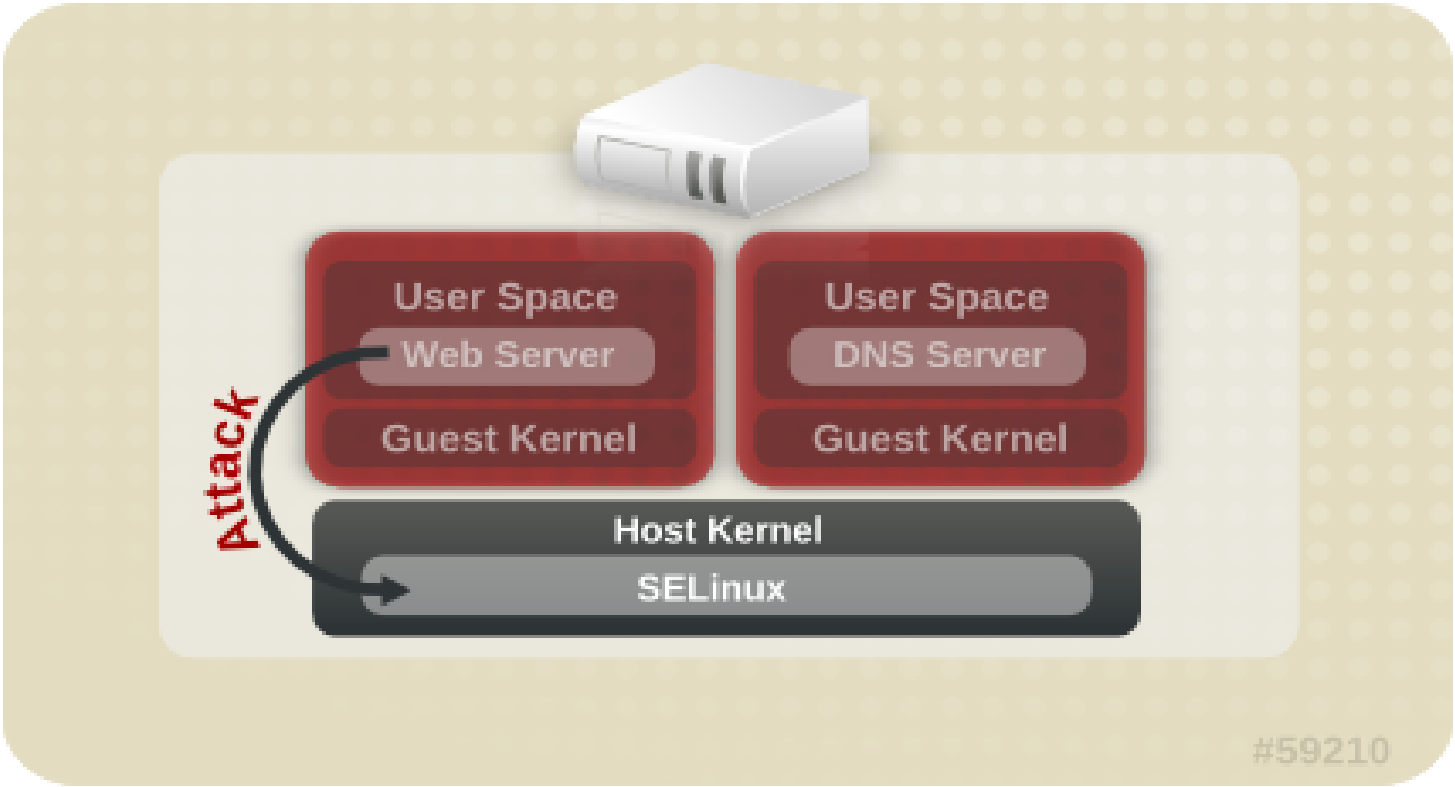
# History : Before Virtualization



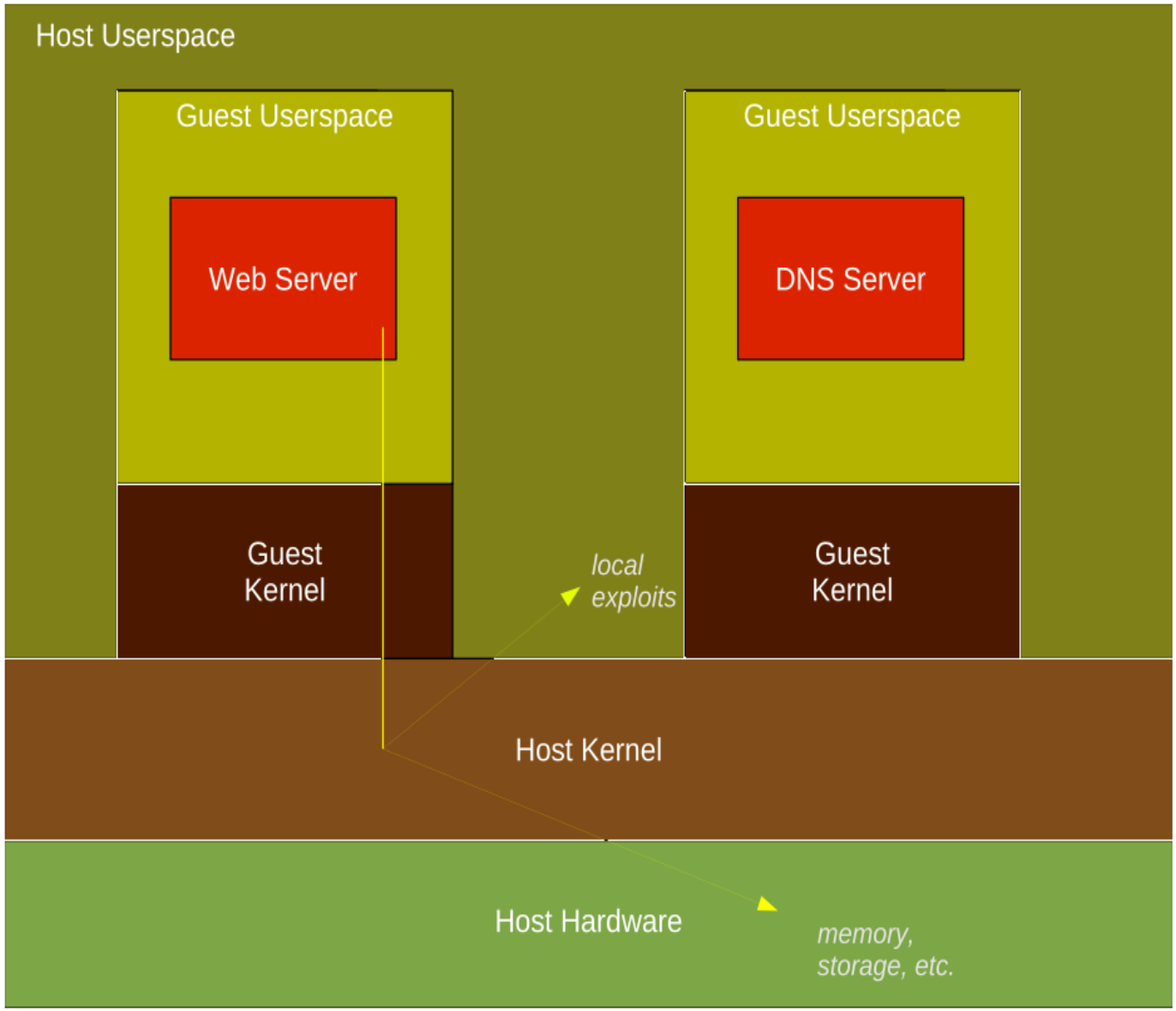
# Present : After Virtualization



# Virtualization Threat



# Internals to threat model



# sVirt : SELinux for libvirt

- Kernel based Manditory Access Control
- Based on SELinux MLS
- Multi-Category Security (MCS)
- Uses libvirt library
- It confines VM's in compartments

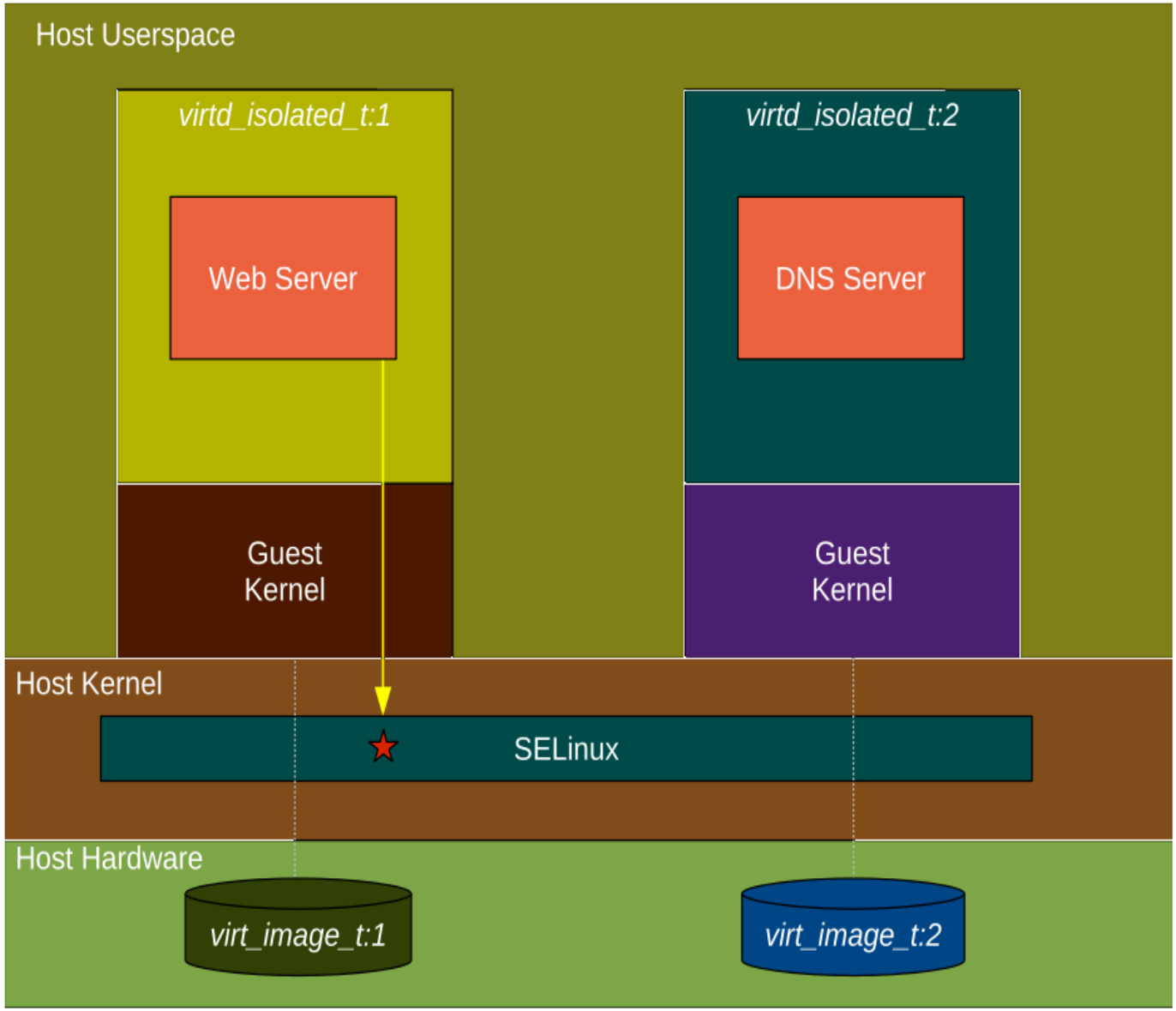
# sVirt Labels (1)

- Processes : system_u:system_r:svirt_t:MCS1
  - MCS1 is a randomly selected MCS field. Currently approximately 500,000 labels are supported.
- Image : system_u:object_r:svirt_image_t:MCS1
  - Only svirt_t processes with the same MCS fields are able to read/write these image files and devices.
- Shared Read/Write Content : system_u:object_r:svirt_image_t:s0
  - All svirt_t processes are allowed to write to the svirt_image_t:s0 files and devices.

# sVirt Labels (2)

- Shared Shared Read Only content : system_u:object_r:svirt_content_t:s0
  - All svirt_t processes are able to read files/devices with this label.
- Image : system_u:object_r:virt_content_t:s0
  - System default label used when an image exits. No svirt_t virtual processes are allowed to read files/devices with this label.

# sVirt model


Host Userspace
virtd_isolated_t:1
Web Server
Guest Kernel
virtd_isolated_t:2
DNS Server
Guest Kernel
Host Kernel
SELinux
Host Hardware
virt_image_t:1
virt_image_t:2

# Labelling VM's

- Label VM images
- Assigning a VM a label

```
<seclabel type='static' model='selinux'>
<label>system_u:system_r:svirt_t:s0:category,category</label>
<imagelabel>system_u:object_r:svirt_image_t:s0:category,category</imagelabel>
</seclabel>
```

- Changing SELinux file label

# 4

# Conclusion

# Conclusion

# The End


Thank You


Toshaan Bharvani - VanTosh bvba
<toshaan@vantosh.com>

http://www.vantosh.com/

Made with Beamer LaTeX
a TeXbased Presentation program