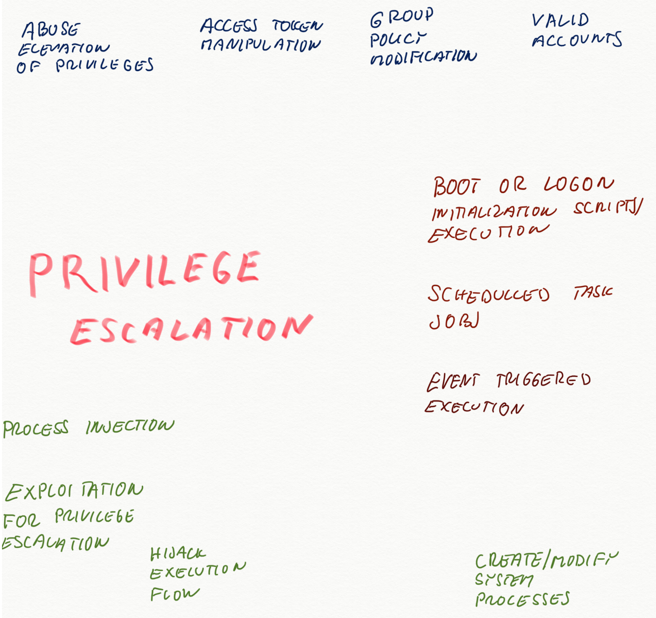
Dealing with untrusted and legacy code: sandboxing and isolation

November 10, 2022

Escalation of privileges


ABUSE ELEVATION OF PRIVILEGES
ACCESS TOKEN MANIPULATION
GROUP POLICY MODIFICATION
VALID ACCOUNTS
BOOT OR LOGON INITIALIZATION SCRIPTS/ EXECUTION
PRIVILEGE ESCALATION
SCHEDULED TASK JOB
EVENT TRIGGERED EXECUTION
PROCESS INJECTION
EXPLOITATION FOR PRIVILEGE ESCALATION
HIJACK EXECUTION FLOW
CREATE/MODIFY SYSTEM PROCESSES

Confinement

The confinement problem deals with prevention of a process to take disallowed actions.

Different levels of confinement

- Air-gap
- Virtual machines
- Sandboxing
- Software Fault Isolation

Isolation based on airgap

Airgaps refers to a system physical detached from network or other means of interaction with other systems.

Bruce Schneier's advices on airgaps

- During set-up use as little internet as possible.
- Turn on encryption.
- Install minimal software you need.
- Once set-up, never connect it to the internet.
- Install only software downloaded anonymously on different computer, check signatures and fingerprints
- Disable all autoruns.
- Minimize the amount of executable code moved to the computer (includes macros in text documents, pdfs).
- Use only trusted media. CDROM is more secure then USB stick. Use the media that just fits your data.
- Consider using stateless OS (Tails).

Bruce Schneier, Schneier on Security, 2013

Covert channels

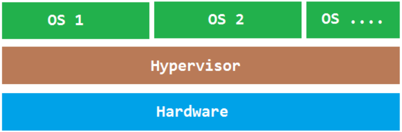
Even airgap can be leapt over using cover channels (electromagnetic radiation, acoustic noise, crt eavesdropping).

Guri, Mordechai, et al. "AirHopper: Bridging the air-gap between isolated networks and mobile phones using radio frequencies, 2014. youtube

IBM 360 — first commercially successful virtualization

By Dave Ross - Flickr: IBM System/360 Model 30, CC BY 2.0, https://commons.wikimedia.org/w/index.php?curid=17268674

Types of virtual machines



OS 1

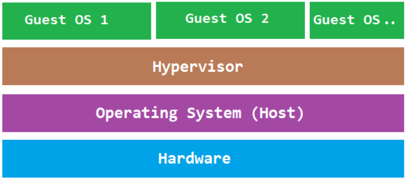
OS 2

OS ....

Hypervisor

Hardware

Type I



Guest OS 1

Guest OS 2

Guest OS..

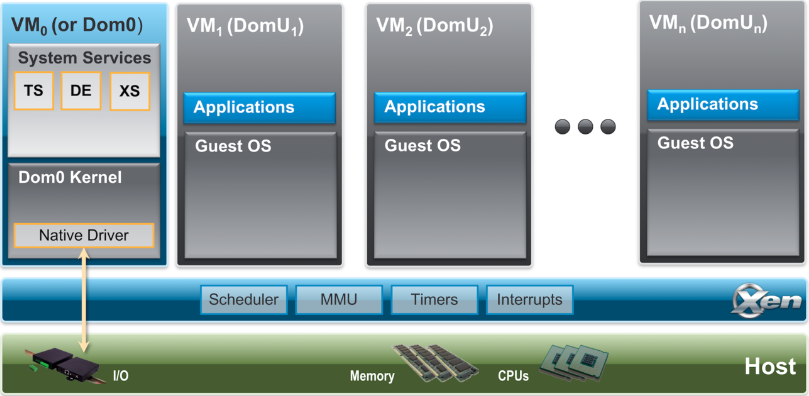
Hypervisor

Operating System (Host)

Hardware

Type II

Xen - paravirtualization



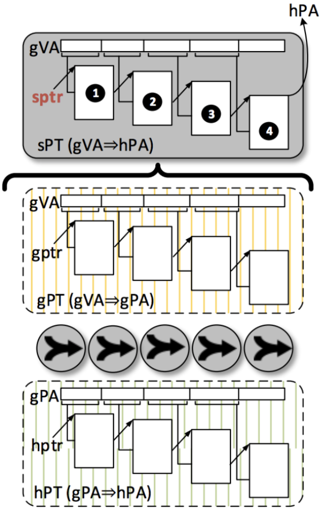
Mechanisms to achieve virtualization

- Separation of memory,
- time-sharing of cpu,
- multi-plexing of IO (network cards, DMA channels, etc.),
- protection of virtual machine monitor.

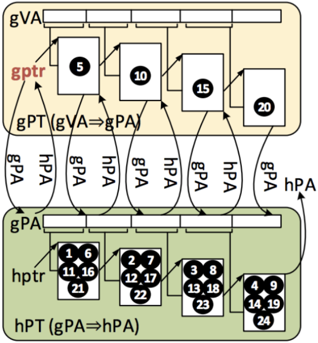
Isolation of memory

- *Guest virtual memory* is visible to applications of guest OS.
- *Guest physical memory* is managed by guest OS.
- *Host virtual memory* is visible to guest OS.
- *Host physical memory* is managed by virtual machine monitor *(machine memory)*.

Isolation of memory

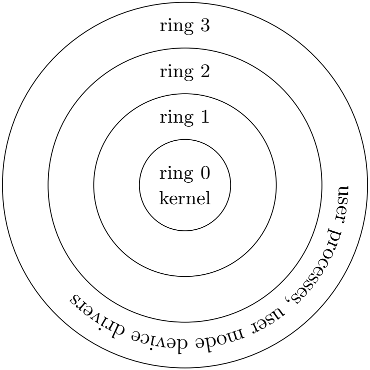


(c) Shadow Paging



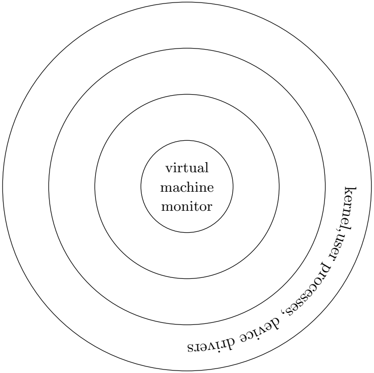
(b) Nested Paging

Isolation of CPU without HW support



Where does *virtual machine monitor* fits in?

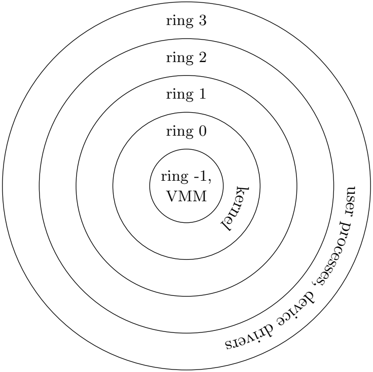
Isolation of CPU without HW support



Ring compression

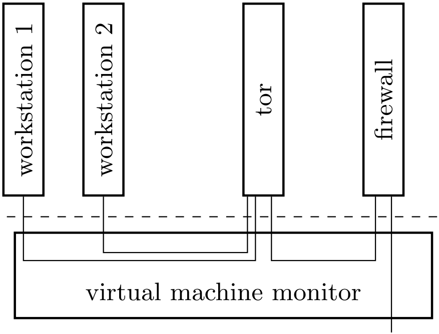
- VMM has access to all resources.
- Privileged instructions are
  - emulated by VMM
  - dynamically recompiled
- guest OS should not know it is in VM.
- What is the impact on kernel being in ring 3?

Isolation of CPU with HW support



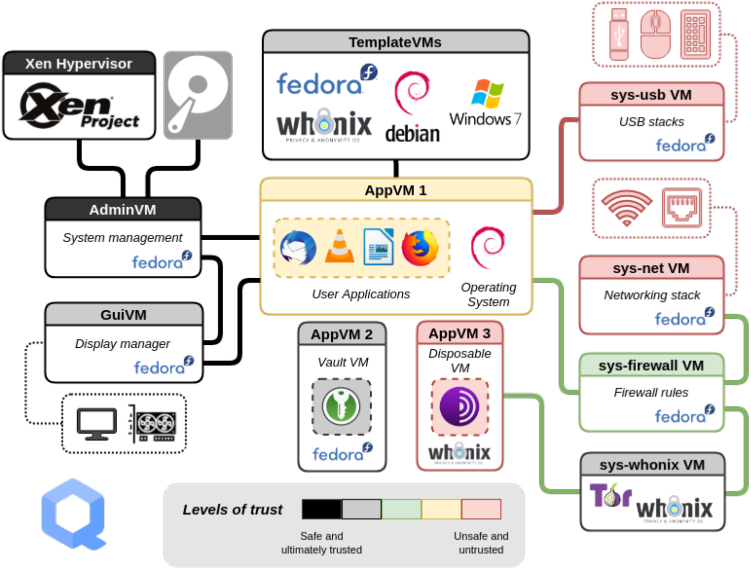
- Added new ring for VM with instructions supporting VMM / VM switch
- VMM in ring -1

Using virtualization to enforce networking rules

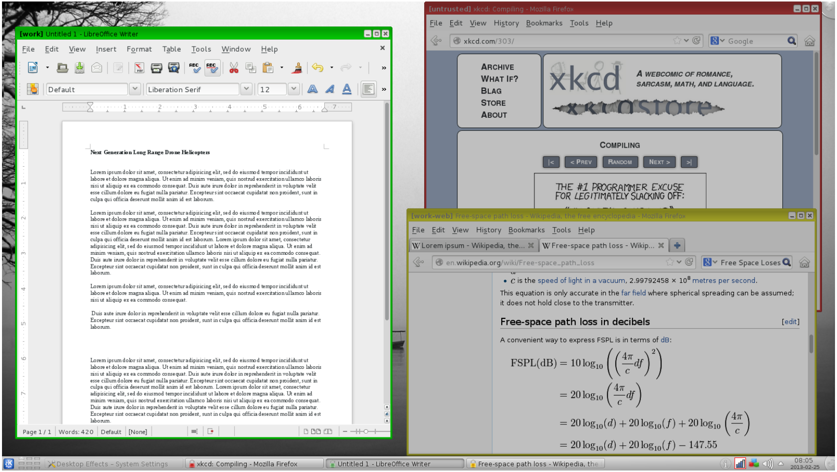


- Dedicated VM communicates with the rest of the world.
- All communication is mediated though firewall / TOR router.
- NSA's NetTop, Qubes-OS, Bromium.

Operating "systems" exploiting virtualization



Operating "systems" exploiting virtualization


[work] Untitled 1 - LibreOffice Writer
File Edit View Insert Format Table Tools Window Help
Default
Liberation Serif
12
Page 1 / 1
Words: 420
Default
[None]
[untrusted] xkcd: Compiling - Mozilla Firefox
File Edit View History Bookmarks Tools Help
xkcd.com/303/
Google
Archive
What If?
Blag
Store
About
xkcd
A webcomic of romance, sarcasm, math, and language.
xkcd store
Compiling
|<
< Prev
Random
Next >
>|
THE #1 PROGRAMMER EXCUSE FOR LEGITIMATELY SLACKING OFF:
[work-web] Free-space path loss - Wikipedia, the free encyclopedia - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Lorem ipsum - Wikipedia, the...
Free-space path loss - Wikip...
en.wikipedia.org/wiki/Free-space_path_loss
Free Space Loses
Desktop Effects - System Settings
xkcd: Compiling - Mozilla Firefox
Untitled 1 - LibreOffice Writer
Free-space path loss - Wikipedia, the
08:05
2013-02-25

Next Generation Long Range Drone Helicopters

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat.

Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum. Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

- c is the speed of light in a vacuum, 2.99792458 × 10^8 metres per second.

This equation is only accurate in the far field where spherical spreading can be assumed; it does not hold close to the transmitter.

Free-space path loss in decibels [edit]

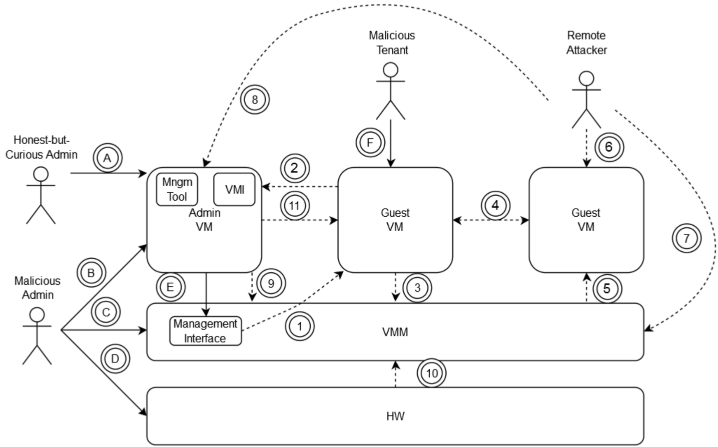
A convenient way to express FSPL is in terms of dB:

$$\begin{aligned}\mathrm{FSPL(dB)} &= 10\log_{10}\left(\left(\frac{4\pi}{c}df\right)^2\right)\\ &= 20\log_{10}\left(\frac{4\pi}{c}df\right)\\ &= 20\log_{10}(d) + 20\log_{10}(f) + 20\log_{10}\left(\frac{4\pi}{c}\right)\\ &= 20\log_{10}(d) + 20\log_{10}(f) - 147.55\end{aligned}$$

Screenshot of Qubes-OS[1]

[1] https://www.qubes-os.org/attachment/wiki/QubesScreenshots/r2b2-kde-three-domains-at-work.png

Attack vector on virtual machines



Evolution of Attacks, Threat Models and Solutions for Virtualized Systems, Daniele Sgandurra and Emil Lupu, 2012

Security issues of virtual machines

- VM sprawl
- Sensitive Data Within a VM
- Security of Offline and Dormant VMs
- Security of Pre-Configured (Golden Image) VM / Active VMs
- Lack of Visibility Into and Controls Over Virtual Networks
- Resource Exhaustion
- Hypervisor Security
- Unauthorized Access to Hypervisor
- Account or Service Hijacking Through the Self-Service Portal
- Workload of Different Trust Levels Located on the Same Server
- Risk Due to Cloud Service Provider API
- The curse of scale