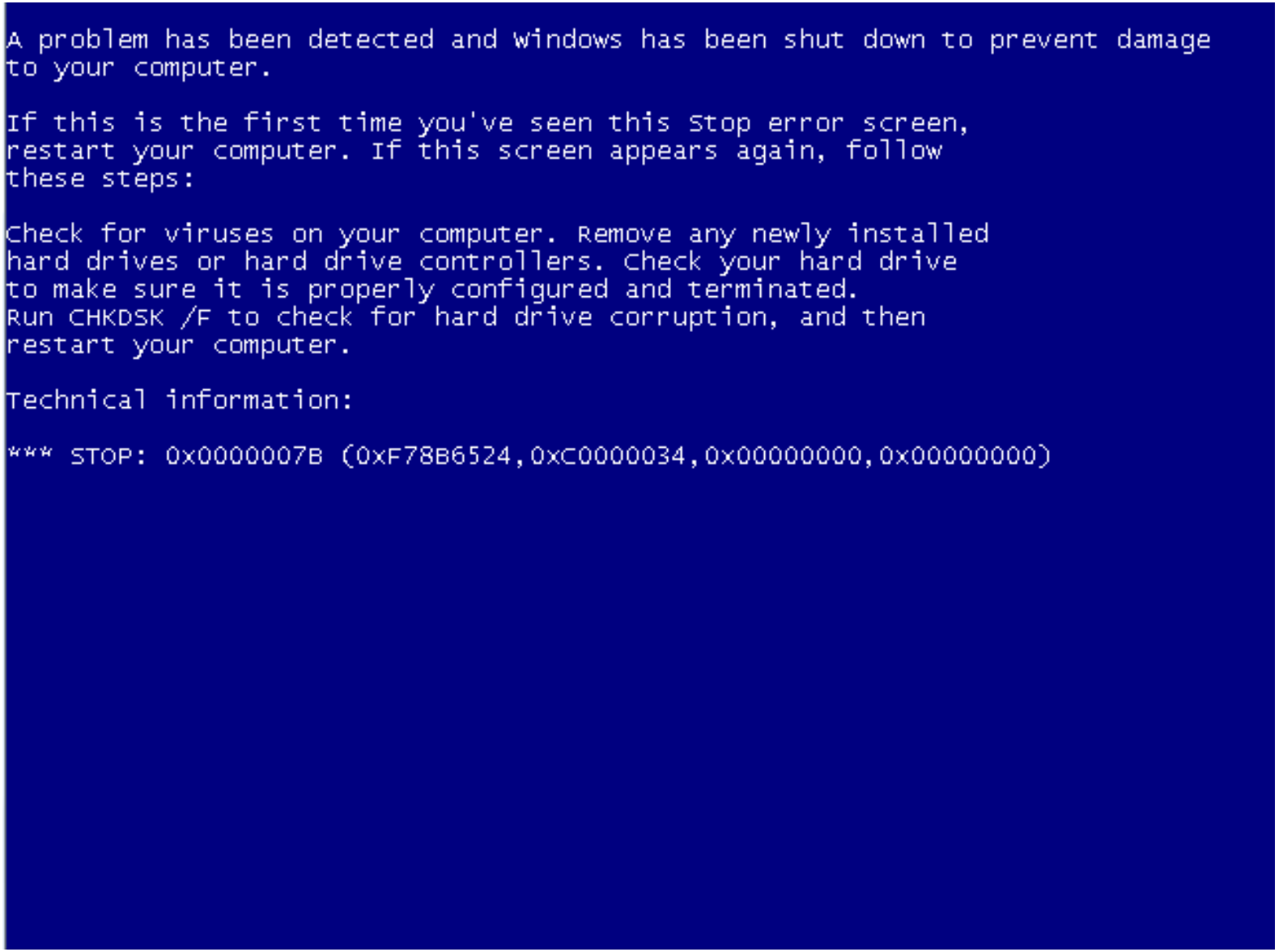
SEGURIDAD EN ENTORNOS VIRTUALIZADOS; EL MODELO DE ANILLOS.

AGUILERA PALACIOS LUIS ERNESTO

¿SEGURIDAD PARA QUÉ?

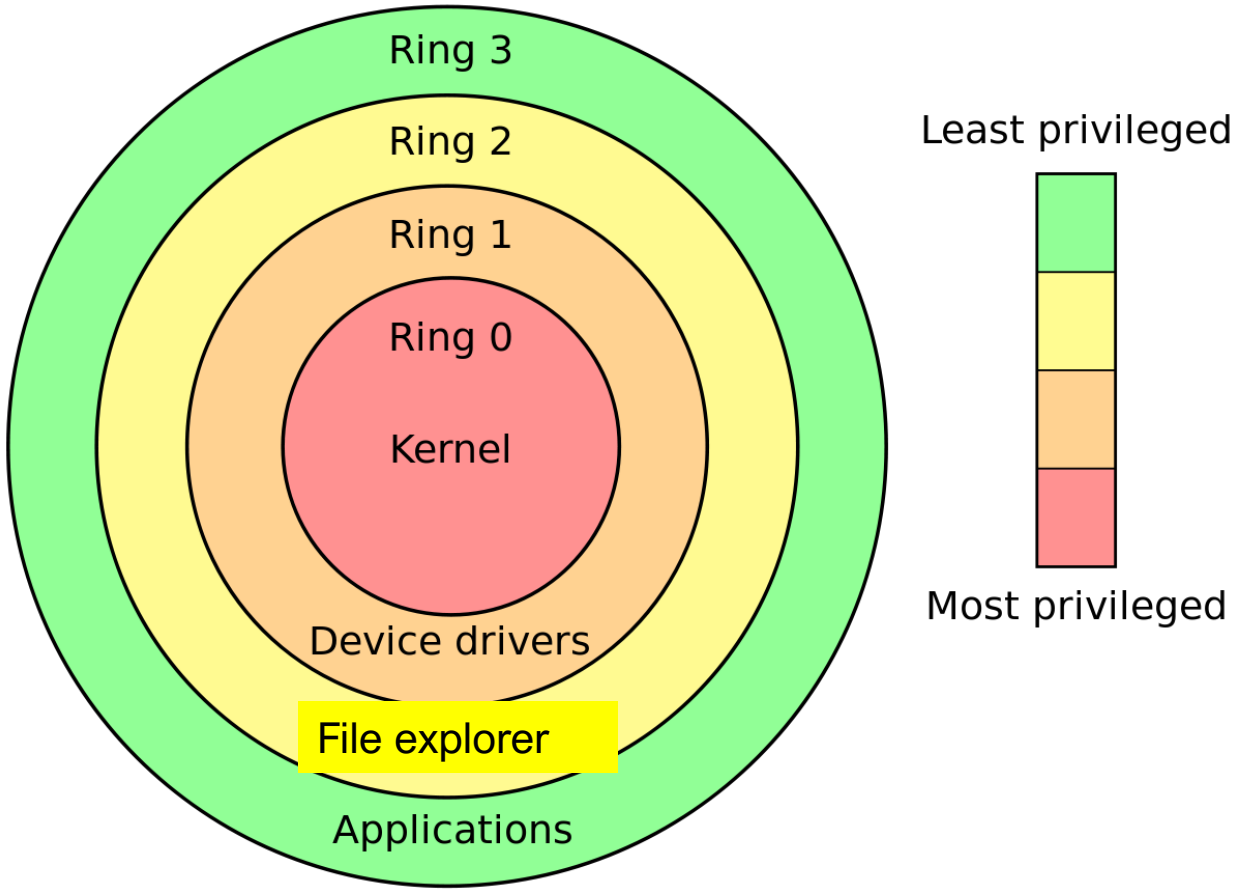
```
[    0.552962] CPU: 3 PID: 1 Comm: swapper/0 Not tainted 4.8.0-44-generic #47~16
.04.1-Ubuntu
[    0.553012] Hardware name: TOSHIBA Satellite C640/Portable PC, BIOS 2.10 11/0
9/2011
[    0.553060]  0000000000000086 0000000064eb1541 ffff9575f4473df0 ffffffffb8a2e
073
[    0.553200]  ffff9575f3ae5000 ffffffffb92725a0 ffff9575f4473e78 ffffffffb879e
6ad
[    0.553341]  ffff957500000010 ffff9575f4473e88 ffff9575f4473e20 0000000064eb1
541
[    0.553482] Call Trace:
[    0.553519]  [<ffffffffb8a2e073>] dump_stack+0x63/0x90
[    0.553562]  [<ffffffffb879e6ad>] panic+0xe4/0x226
[    0.553606]  [<ffffffffb9586540>] mount_block_root+0x1fb/0x2c2
[    0.553647]  [<ffffffffb958663a>] mount_root+0x33/0x35
[    0.553688]  [<ffffffffb9586776>] prepare_namespace+0x13a/0x18f
[    0.553731]  [<ffffffffb95861eb>] kernel_init_freeable+0x1ee/0x217
[    0.553775]  [<ffffffffb8e8d2ae>] kernel_init+0xe/0x100
[    0.553817]  [<ffffffffb8e9aa1f>] ret_from_fork+0x1f/0x40
[    0.553858]  [<ffffffffb8e8d2a0>] ? rest_init+0x80/0x80
[    0.553932] Kernel Offset: 0x37600000 from 0xffffffff81000000 (relocation ran
ge: 0xffffffff80000000-0xffffffffbfffffff)
[    0.553991] ---[ end Kernel panic - not syncing: VFS: Unable to mount root fs
 on unknown-block(0,0)

_
```


A problem has been detected and windows has been shut down to prevent damage
to your computer.
If this is the first time you've seen this Stop error screen,
restart your computer. If this screen appears again, follow
these steps:
Check for viruses on your computer. Remove any newly installed
hard drives or hard drive controllers. Check your hard drive
to make sure it is properly configured and terminated.
Run CHKDSK /F to check for hard drive corruption, and then
restart your computer.
Technical information:
*** STOP: 0x0000007B (0xF78B6524,0xC0000034,0x00000000,0x00000000)

Cuando un error sucede en un programa que se ejecuta en **modo usuario** el único problema que suele causar es la inconveniencia para quien lo estaba utilizando. Pero si ese mismo error sucede en un programa que corre con **privilegios de root** las consecuencias son incluso peores: se podría llegar a producir un ***Kernel Panic*** o, dicho de otra forma, **la parada súbita de la máquina en la mayoría de situaciones; el error más grave que se puede generar en Unix.**

https://www.ibiblio.org/pub/Linux/docs/LuCaS/Manuales-LuCAS/SEGUNIX/unixsec-2.1.pdf



NIVELES DE SEGURIDAD

¿Qué son los anillos de seguridad?

Los anillos de seguridad hacen referencia a los **mecanismos de protección de datos** que están presentes **ante un fallo o comportamiento malicioso.** Es por esto que los sistemas operativos proporcionan **diferentes niveles de acceso a los recursos**.

Los anillos están superpuestos en una jerarquía de la más privilegiada (de mayor confianza, por lo general numerado cero) a la menos privilegiada (de menor de confianza, por lo general con el número más alto de la enumeración de capas). En la mayoría de los sistemas operativos, el anillo 0 es el nivel con la mayoría de los privilegios e interactúa más directamente con el hardware físico, como la CPU y la memoria. Aunque en principio el nivel cero representa el nivel con más confianza, más adelante se introducirá el concepto de anillo -1.

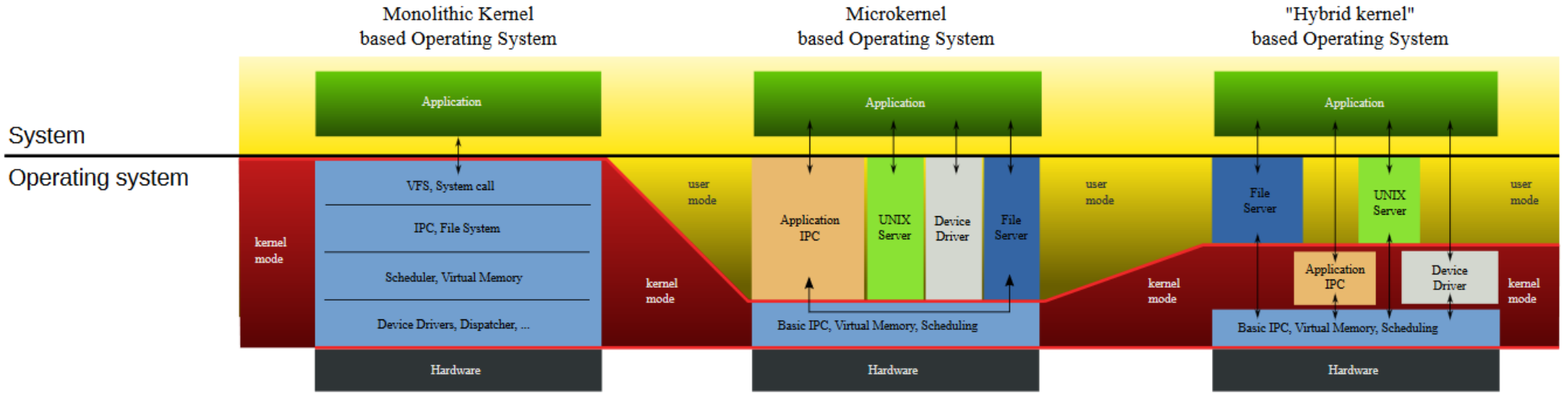
http://mx.globedia.com/capas-anillos-seguridad-nucleo-windows

¿Por qué se implementan diferentes anillos de seguridad?

La idea de múltiples anillos de protección nació con el sistema operativo ***Multics***, predecesor de la actual familia Unix, el cual implementaba 8 anillos. Y en la actualidad la familia Windows (Windows 8 y sus predecesores) utilizan sólo dos anillos que corresponde a los modos disponibles, el anillo 0 correspondiente al modo núcleo y el anillo de 3 correspondiente al modo de usuario.

El uso eficaz de la arquitectura de anillo requiere una estrecha cooperación entre el **hardware y el sistema operativo**. Sin embargo los sistemas operativos diseñados para funcionar en múltiples plataformas de hardware pueden hacer un uso de un número limitado de anillos si no están presentes en todas las plataformas compatibles. **A menudo**, el modelo de seguridad **se simplifica a "kernel" y "usuario",** incluso si el hardware proporciona granularidad más fina a través de los anillos.

http://mx.globedia.com/capas-anillos-seguridad-nucleo-windows


Monolithic Kernel
based Operating System
Microkernel
based Operating System
"Hybrid kernel"
based Operating System
System
Operating system
Application
Application
Application
kernel
mode
VFS, System call
IPC, File System
Scheduler, Virtual Memory
Device Drivers, Dispatcher, ...
Hardware
user
mode
kernel
mode
Application
IPC
UNIX
Server
Device
Driver
File
Server
Basic IPC, Virtual Memory, Scheduling
Hardware
user
mode
kernel
mode
File
Server
UNIX
Server
Application
IPC
Device
Driver
Basic IPC, Virtual Memory, Scheduling
Hardware
user
mode
kernel
mode

Modo Supervisor

Privilegio asociado a un proceso para realizar determinadas acciones dentro del funcionamiento de un sistema operativo.

Todas las tareas a nivel de sistema y sus *threads* (hilos) tendrán éste indicador activado, por lo cual podrían realizar operaciones a bajo nivel. Sin embargo las aplicaciones que corran en el espacio de usuario no podrán realizar esto.

Un modo supervisor es de confianza nunca debe fallar, ya que un error suyo puede hacer que todo el sistema de equipo se bloquee.

http://mx.globedia.com/capas-anillos-seguridad-nucleo-windows

Modo Hypervisor

Se trata de una plataforma que permite aplicar diversas técnicas de control de virtualización para utilizar, al mismo tiempo, diferentes sistemas operativos en un mismo equipo. Es una extensión de un “supervisor”.

http://mx.globedia.com/capas-anillos-seguridad-nucleo-windows

Los hipervisores pueden clasificarse en dos tipos:

Hipervisor tipo 1: También denominado **nativo**, es software que se ejecuta directamente sobre el hardware, para ofrecer la funcionalidad descrita. Ejemplo: VMware ESX (de pago), *Microsoft Hyper-V Server (gratis)*.

Hipervisor tipo 2: También denominado **hosted**, es software que se ejecuta sobre un sistema operativo para ofrecer la funcionalidad descrita. Como ejemplo se puede tener VirtualBox (gratis), VirtualBox OSE (libre), VMware: Workstation (de pago), Server (gratis), *Virtual PC*

http://mx.globedia.com/capas-anillos-seguridad-nucleo-windows

Hypervisor Design:

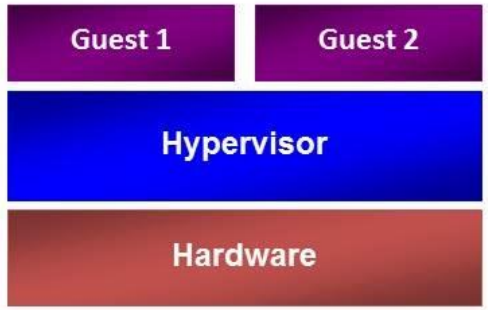
Two approaches

Type 2 Hypervisor

Examples:

- Virtual PC & Virtual Server
- VMware Workstation
- KVM

Type 1 Hypervisor



Examples:

- Hyper-V
- Xen
- VMware ESX

Una ayuda del hardware: SVM, VT-x y SLAT

La traducción de direcciones de segundo nivel (SLAT), también conocida como paginación anidada, es una **tecnología de virtualización asistida por hardware** que **permite evitar los gastos generales asociados con las tablas de páginas de sombra administradas por software.**

AMD ha apoyado a SLAT a través de **la tecnología *Rapid Virtualization Indexing* (RVI)** desde la introducción de sus procesadores Opteron de tercera generación (nombre en clave Barcelona). La implementación de SLAT de **Intel, conocida como *Extended Page Table* (EPT),** se introdujo en la microarquitectura Nehalem que se encuentra en ciertos procesadores Core i7, Core i5 y Core i3.

https://en.wikipedia.org/wiki/Second_Level_Address_Translation

Las extensiones de virtualización de ARM son compatibles con SLAT, conocidas como tablas de páginas de Etapa-2 proporcionadas por una MMU de Etapa-2. El invitado utiliza el MMU de Etapa-1. El soporte se agregó como opcional en la arquitectura ARMv7ve y también se admite en las arquitecturas ARMv8 (32 bits y 64 bits).

Las soluciones en las arquitecturas x86 de Intel y AMD son VT-x y AMD-V(también conocido como SVM), las cuales son las predecesoras de las actuales tecnologías SLAT.

https://en.wikipedia.org/wiki/Second_Level_Address_Translation

El problema con la escalación de privilegios

La escalación de privilegios es muy común en ataques cibernéticos contra infraestructuras computacionales pues cuando logramos pasar de *ring 3* a *ring 0* (o mejores), el sistema queda prácticamente a nuestra merced como atacantes.

Por ello se debe poner especial cuidado a los mecanismos que implementaremos para cuidar los recursos de nuestro sistema.

El BIOS/UEFI

- You can read about Intel Xeon security features at: https://www.intel.com/content/www/us/en/data-security/security-overview-generaltechnology.html
    1. Identity-protection technology
    2. Advanced Encryption Standard New Instructions
    3. Trusted Execution Technology
    4. Hardware-assisted virtualization technology

- And, you can read about AMD EPYC security features at https://semiaccurate.com/2017/06/22/amds-epyc-major-advance-security/
    1. Secure Memory Encryption
    2. Secure Encrypted Virtualization

Bibliografía

- Seguridad en Unix y Redes Antonio Villalon Huerta Versión 2.1 Julio de 2002
- Mastering Linux: Security and Hardening Donald A. Tevault 1a Edición Enero de 2018