Universidad Nacional Autónoma De México

Facultad de Ingeniería

Sistemas operativos

Exposición 02

Seguridad en Entornos virtualizados; el modelo de anillos.

Aguilera Palacios Luis Ernesto

07/03/2019

Kernel Panic

El error más crítico en un Sistema UNIX es el *kernel panic*.

El modelo de anillos

Los kernels modernos de prácticamente todos los sistemas operativos incluyen el manejo de al menos dos anillos de seguridad, estos nos permiten tener varios niveles de privilegios.

Entornos virtualizados: el modo supervisor

El modo supervisor es la primera aproximación que se dio al problema de la administración de recursos en los grandes mainframes de los años 60s.

Entornos virtualizados: el modo hypervisor

El modo hypervisor nace como respuesta a los nuevos desafíos que representaba la virtualización a principios del milenio.

Una ayuda del hardware

Viendo los retos y el costo que supone la virtualización, las grandes compañías de hardware comienzan a pensar en una solución que permita reducir dichos costos computacionalmente.

Introducción:
¿Y la seguridad para qué?

Algunos de los retos

Evitar la canibalización de recursos.

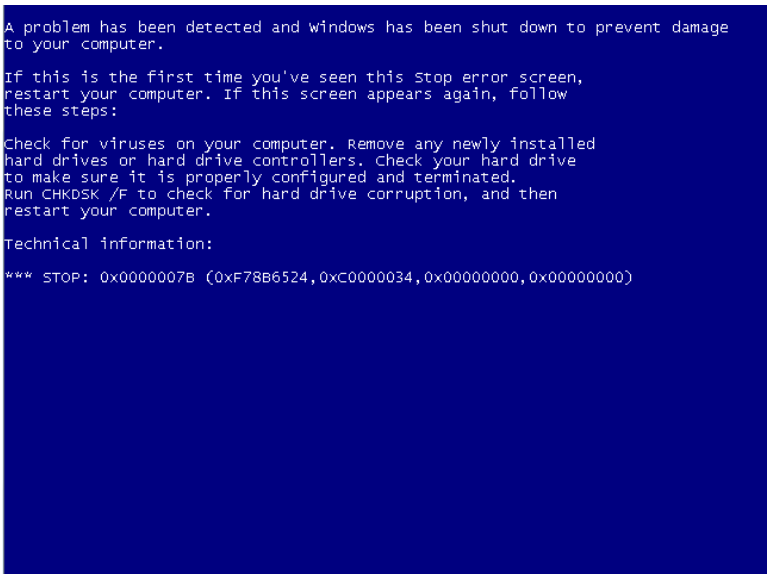
Los servidores en la nube deben delimitar muy bien cuáles recursos le pertenecen a cada usuario o grupo de usuarios.

Prevenir la fuga de información.

Muchos de estos servidores alojan información sensible que debe ser visible sólo para las personas y/o sistemas autorizadas.

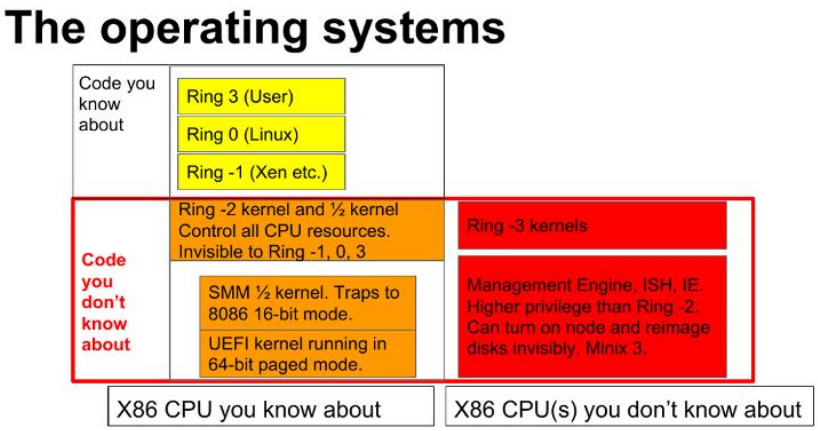
Dentro de la computación en la “nube” la seguridad ha sido uno de los principales retos a vencer, y a pesar de que en los últimos años hemos logrado superar problemas de potencia y escalabilidad, la seguridad sigue planteando un muro bastante duro de derribar, pues empezando por el control de los recursos estos ya suponen un cambo con respecto al cómputo personal que plantea nuevas perspectivas e ideas.

Kernel Panic



En la mayoría de los casos un programa no debería poner en un punto de parada súbita a la máquina sobre la que se ejecuta, cuando esto sucede generalmente es por que dicho programa se ha ejecutado en modo supervisor, kernel o privilegiado, y ha fallado; a esto se le conoce como Kernel Panic y es bastante catastrófico desde el punto de vista de la máquina por que ni siquiera el mismísimo kernel puede corregir dicha situación, teniendo que recurrir a reiniciar el sistema cada vez que suceda.

El modelo de anillos



Multics fue el primer sistema operativo en introducir el concepto de acceso por anillos, Multics poseía un total de 8 anillos de acceso, el anillo 0 es el del kernel y el de mayor confianza mientras que el anillo 7 era el de menor confianza, posteriormente las arquitecturas Mips y PowerPC introdujeron un soporte para sólo dos anillos de protección, con lo cuál muchos sitemas operativos modificaron sus núcleos para operar en ellos, quedando sólo el anillo 0 (modo kernel) y el anillo 3 (modo usuario). Aunque con el paso del tiempo se han introducido nuevos niveles, estos no son ampliamente conocidos y muchos manejan sólo dos anillos de protección.

Cada anillo es un nivel nuevo de seguridad que implementa el sistema operativo para poder proteger recursos, archivos y otros componentes de nuestras máquinas, para pasar de un anillo a otro se hace uso de un modelo proxy, lo que quiere decir que no podemos acceder directamente a los recursos que están a cargo del siguiente anillo, si no que tenemos que solicitar el acceso y este será restringido.

Entornos virtualizados: El supervisor

Con el supervisor nos referimos a un modo de acceso que mediante una bandera intenta controlar el acceso a los recursos y procesos, este enfoque viene desde los años en que se utilizaban mainframes para desarrollar trabajos computacionales y el tiempo compartido era una necesidad más que una opción, entonces para garantizar un uso justo para todos los usuarios se desarrollaban estos supervisores que verificaban entre otras cosas: el tiempo de uso, la cantidad de memoria que cada uno tenía disponible, etc.

Cuando la potencia computacional aumento rápidamente entre los 80-90s también lo hicieron los problemas y huecos de seguridad que iba dejando a su paso, por ejemplo ahora era posible hacer condiciones de carrera para ganar acceso a recursos protegidos o escalar privilegios a *ring 0,* otro problema que se descubrió en esa época fue el *buffer overflow* que hasta nuestro días sigue causando dolores de cabeza, pues permite escapar de un sector de la memoria y direccionar más memoria de la permitida.

Entornos virtualizados: El hypervisor

Cuando los supervisores comenzaron a ser insuficientes para vigilar un sistema que cada vez era más complejo, se desarrollaron los hypervisores que son una extensión de los anteriores, pero ahora tenían distintas técnicas que les permitían monitorizar más cosas al mismo tiempo, estos fueron pensados principalmente para virtualizar de manera más eficiente y controlada.

Exiten dos tipos de hypervisores los nativos, que son una implementación de software que levanta un nivel extra de anillo(-1) para poder administrar los recursos de todas las máquinas corriendo incluida la principal. La otra es el hosted, estos hypervisores corren sobre el sistema operativo anfitrión y de este modo el hypervisor queda por debajo del SO principal en nivel de privilegios.

Una ayuda del hardware

Los hypervisores habían resuelto el problema de la administración de recursos, pero habían dejado otro abierto; la eficiencia. Dado que cada cambio de anillo implica una llamada al sistema y esta implica un cambio de contexto, los hypervisores tuvieron un inicio difícil, pero gracias al interés por su utilidad para el cómputo “en la nube” y los servidores profesionales, estos obtuvieron el apoyo de los fabricantes de hardware en forma de hardware dedicado a optimizar la gestión y seguridad de los hypervisores.

La tecnología más destacable que desarrollaron para este propósito fue SLAT o Traducción de direcciones de segunda capa por sus siglas en inglés, que permite hacer la paginación de la memoria virtual de un modo alrededor de 40% más rápido que las soluciones por software.

Bibliografía:

- Mastering Linux: Security and Hardening Donald A. Tevault 1a Edición Enero de 2018
- Seguridad en Unix y Redes Antonio Villalon Huerta Versión 2.1 Julio de 2002
- AMD Inc. Julio, 2008 AMD-V Nested Paging. 07 de Marzo de 2019 de: https://web.archive.org/web/20120905060541/http://developer.amd.com/assets/NPT-WP-1%201-final-TM.pdf
- http://mx.globedia.com/capas-anillos-seguridad-nucleo-windows