# SISTEMAS VIRTUALIZACION Y SEGURIDAD

FEBRERO 2022

## PREGUNTA 1 INTRODUCCION Y RENDIMIENTO (1 PUNTOS)

a) ¿De las diversas configuraciones de *SpecCPU* cuando no es ventajoso disponer de múltiples CPUs en el sistema bajo test (i.e. añadir más CPUs no mejora el comportamiento)?
b) Explicar la/s diferencia/s entre los "*Client*" y el "*PrimeClient*" de *SpecWeb2005*
c) ¿Qué modela el *benchmark* SpecJbb 2005?
d) ¿Cuál es la diferencia entre *peak* y *base* en *SpecCPU*?

## PREGUNTA 2 CLOUDS PUBLICOS Y CONTAINERS (1.5 PUNTO)

*a)* ¿En que condiciones disponer de servidores *on-premises* es económicamente ventajoso con respecto a emplear servidores en el *cloud?*
b) ¿Cuál es la utilidad de disponer de *containers* no privilegiados en un sistema que hemos de administrar?
c) ¿En que consiste los *overlayFS* que emplean *lxc* y *docker*?
d) ¿Cómo se elimina una imagen en *docker*? ¿Y un contenedor *docker*?
*e)* ¿Cómo se puede ejecutar un contenedor *docker* en un host Windows?

## PREGUNTA 3 MÁQUINAS VIRTUALES (1.5 PUNTOS)

a) ¿Cuál es la diferencia entre *hipervisor* y *Virtual Machine Monitor* (VMM)?
b) Según el teorema de *Popek* y *Goldberg*, ¿En que condiciones un ISA es virtualizable recursivamente?
c) ¿Cuáles son posibles alternativas a la hora de implementar la virtualización a nivel de sistema?
d) ¿Cómo se previene en *VMWare* que el *guest* acceda al *VMM*?
e) ¿Para qué sirve el *Memory Tracing* que emplea VMWare?

## PREGUNTA 4 SOPORTE ARQUITECTURAL VIRTUALIZACION MEM Y CPU (1.5 PUNTOS)

a) ¿Por qué diferentes implementaciones de x86 las instrucciones asociadas a VT-x tienen un rendimiento diferente (tendiendo a ser más rápidas en los procesadores más recientes)?
b) ¿En términos de rendimiento, que implica un *vmexit* en VT-x?
c) ¿Por que razón en un sistema dado x86 puede ser posible crear máquinas virtuales *VirtualBox* de 32-bits pero no de 64-bits?
d) ¿Por qué no es posible aplicar las ideas de *Xen* en *VMWare* (teniendo en cuenta los objetivos de diseño de ambos)?
e) ¿Por qué diferentes tamaños de páginas en las EPT pueden tener un efecto significativo en el rendimiento del sistema? ¿Qué aplicaciones serán más sensibles?

## PREGUNTA 5 ENTRADA SALIDA (1.5 PUNTOS)

a) En sistema VDI (*Virtual Desktop Infraestructure*), el empleo de drivers paravirtualizados mejora substancialmente la experiencia de usuario ¿Por qué?
b) En un servidor moderno, ¿Dónde se encuentra la IOMMU y cuál es su utilidad?
c) Explicar brevemente como funciona la interposición de entrada salida y por que no es necesaria en un dispositivo de I/O y sistema con SRIOV

d) ¿Por qué *kvm* hace una excepción con la paravirtualización de la red (y en que consiste la excepción)?

e) ¿En que condiciones la virtualización de entrada salida no tiene ningún *overhead*?

## PREGUNTA 6 INTRO SEGURIDAD (1.5 PUNTOS)

*a)* ¿Por qué tiene poco sentido evitar mejorar la seguridad del TCB ocultado su implementación? ¿Qué ejemplos recientes conoces que afrontan este problema?

b) ¿Cuál es la diferencia entre confidencialidad e integridad?

c) ¿Desde el punto de vista de la privacidad del usuario, es mejor la idea de los enclaves seguros (e.g. Intel SGX) o la de el cifrado completo en memoria (e.g. Amd SEV)?

d) ¿Cuál es la diferencia entre SMM (ring-2) y SecE (ring -3)?

e) ¿Cómo se puede modificar el firmware del TCB (e.g. para corregir un bug) de forma segura?

## PREGUNTA 7 PRACTICO SEGURIDAD (1.5 PUNTOS)

a) Explicar cómo funcionan los ataques tipo Spectre y justificar su peligrosidad. ¿Qué soluciones existen para defendernos de ellos?

b) ¿Por qué es necesario emplear *cifrado* y *hashing* en memoria para garantizar que su contenido sea seguro?

c) En un sistema multiprocesador, ¿Cómo podemos lograr que todos los controladores de memoria empleen la misma clave de cifrado para una máquina virtual dada?

d) Citar un ejemplo de utilidad del sealing y explicar como funciona.

e) ¿Cuál es el "medio" de fuga (i.e. *channel*) que emplean los ataques laterales (i.e. *Side-channel attacks*) que explotan la ejecución especulativa de instrucciones en los procesadores modernos?