SISTEMAS VIRTUALIZACION Y SEGURIDAD

FEBRERO 2021

PREGUNTA 1 INTRODUCCION Y RENDIMIENTO (1 PUNTOS)

a) ¿Por qué las tecnologías de virtualización juegan un papel fundamental en el Cloud Computing? ¿En que capa del Stack se encuentran?

b) ¿Cuál es la razón de ser de los *Clouds* híbridos?

c) Explicar los elementos que forman parte de la suite SpecWeb2005. Describir un sistema (HW y SW) que pudiese lograr maximizar el rendimiento obtenido.

d) ¿Cuales son los posibles tamaños de problema en las aplicaciones de *SpecCPU2017*? ¿Cuál es la utilidad de cada uno de ellos?

PREGUNTA 2 CLOUDS PUBLICOS Y CONTAINERS (2 PUNTOS)

a) ¿Por qué los *overheads* en CPU o memoria que conlleva el uso de contenedores es inferior al de las máquinas virtuales?

b) ¿Un contenedor es más seguro que una máquina virtual? ¿Por qué?

c) ¿Cual es la mejor opción, desde el punto de vista de seguridad, a la hora de instalar un *docker* prediseñado, como el que ofrecen los desarrolladores de *gitlab*?

d) ¿Cuál es el proceso de creación desatendido de un contenedor tipo "*docker*"? ¿Cómo se puede acceder a un contenedor (en ejecución)? ¿Y a una imagen?

e) ¿Cuál es el modo más económico de mantener una máquina virtual en GCE? ¿Por qué es más económico que el modo normal?

f) Explicar cual es la utilidad de *DockerSwarm*. ¿Conoces alguna alternativa?

PREGUNTA 3 MÁQUINAS VIRTUALES (2 PUNTOS)

a) ¿Qué ventajas y desventajas presenta un sVM tipo-1 frente a una tipo-2? Citar dos ejemplos de cada tipo.

b) Según el teorema de *Popek y Goldberg*, ¿Qué diferencia las máquinas virtuales de los simuladores? (y por que dicho teorema no es aplicable a los simuladores)

c) ¿Cómo se logra virtualizar ISAs en los que todas las instrucciones sensibles al comportamiento y al control no son privilegiadas? Citar un ISA y explicar una instrucción de este este tipo. ¿Por qué crees que en el diseño del ISA se pueden llegar a tomar esas decisiones (tan contraproducentes)?

d) ¿Por qué del ISA del MIPS es, en principio, no virtualizable? ¿Cómo resolvía este contratiempo DISCO?

e) ¿Qué contiene la Cache de traducciones (o TC) usado en las versiones VMWare ideadas para una arquitectura x86 sin soporte arquitectural para virtualización?

f) ¿Cuál es papel del componente VMX en VMWare?

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

a) ¿Qué mecanismo se emplea para comunicar el hipervisor (p.ej. kvm) con las extensiones de virtualización VT-x? ¿Qué papel juega *QEMU* en *kvm*?

b) ¿Por qué en versiones iniciales del VT-x, su uso podía llegar a ser contraproducente (i.e. el uso de Hipervisores que no hicieran uso de VT-x podían alcanzar una virtualización con menor *overhead*)

c) ¿Por qué una configuración incorrecta de las EPT (p.ej. usar paginas en EPT demasiado pequeñas) pueden afectar incrementar el *overhead* de la virtualización?

d) ¿Cómo se virtualiza el TLB en un sistema en el que no esta expuesto a la arquitectura (*architected*)? ¿Cómo se resuelve el problema en x86 en la primera y segunda generación de VT-x?

PREGUNTA 5 ENTRADA SALIDA (1.5 PUNTOS)

a) ¿Como se identifica unívocamente cada dispositivo en un bus PCIe?
b) ¿Por qué es más eficiente la paravirtialización de los dispositivos I/O que su emulación? ¿Qué limitaciones tiene la paravirtualización?
c) ¿Qué excepción (con respecto a otros dispositivos de I/O) se realiza en Linux con la paravirtualizacion de los dispositivos de red?
d) ¿Qué ventajas presentan los dispositivos SRIOV? ¿Qué limitaciones tiene un controlador de interrupciones no virtualizado (como APIC en x86) cuando se emplean dispositivos SRIOV?

PREGUNTA 6 SEGURIDAD (2 PUNTOS)

a) ¿Donde se ejecutan el TCB y el TEE?
b) Explicar las diferencias entre un *Cover Channel* y un *Side Channel*, en el contexto de seguridad. Citar un ejemplo de ambos.
c) ¿Que es el *Hardware Root of Trust* y en que condiciones es vulnerable?
d) ¿Cual es la diferencia entre Sellado (*Sealing*) y Medida (*Measurement*)?
e) ¿Por qué es necesario garantizar la integridad de los datos en memoria? ¿Cómo se puede hacer?
f) Explicar como funciona los ataques tipo *Spectre* y justificar su peligrosidad. ¿Qué soluciones existen para defendernos de ellos?