

Explotando Vulnerabilidades en Consolas de Videojuegos

Cómo las consolas se convierten en
objetivos para los ciberatacantes

Jose Fernández López



whoami

- ~~Pasión por el Diseño Gráfico~~
- (Casi) Ingeniero
- Investigador en Univ. Alcalá (Cátedra IA)
- Otros proyectos
- No juego a videojuegos
- DNI: 59647307G
- Num. Seg. : 09 – 9109515580
- Tarjeta: 4373054386065039
- Caducidad: 10/24
- CVV: ***



Jose Fernández

¿Consolas? No solo sirven para jugar

Hay un lado oscuro detrás de ellas...

- ¿Se pueden hackear? Pues como cualquier cosa...
- ¿Y si las usamos para el mal?
- La piratería no es interesante (Ni legal)
- El Bug Bounty no da para comer



Las consolas antes

Antes



- Trozo de plástico
- Sin puertos de entrada
- Solo podías piratear juegos

Las consolas ahora

- Super potentes
- Nuevas formas de interactuar...

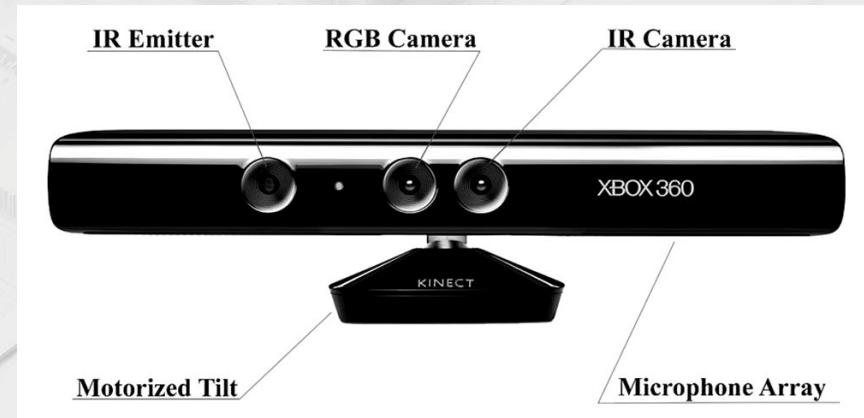


Ahora



Ejemplo: Xbox Kinect

- Primeras controversias
- Cámaras (+ visión nocturna)
- Sensores de posición
- Reconocimiento facial
- Micrófonos
- Detector de pulsación



Xbox Kinect ❤️ NSA

(Caso real)

- Utilizaban Kinect para espiar
- Se aprovechaban de vulnerabilidades
- Otros usuarios las descubrieron...
- Si la NSA puede, tu también

libfreenect

libfreenect is a userspace driver for the Microsoft Kinect. It runs on Linux, OSX, and Windows and supports

- RGB and Depth Images
- Motors
- Accelerometer
- LED
- Audio

Xbox, Kinect NSA Spying Was Done Without Consent, Claims Microsoft

News By Will Usher published December 9, 2013

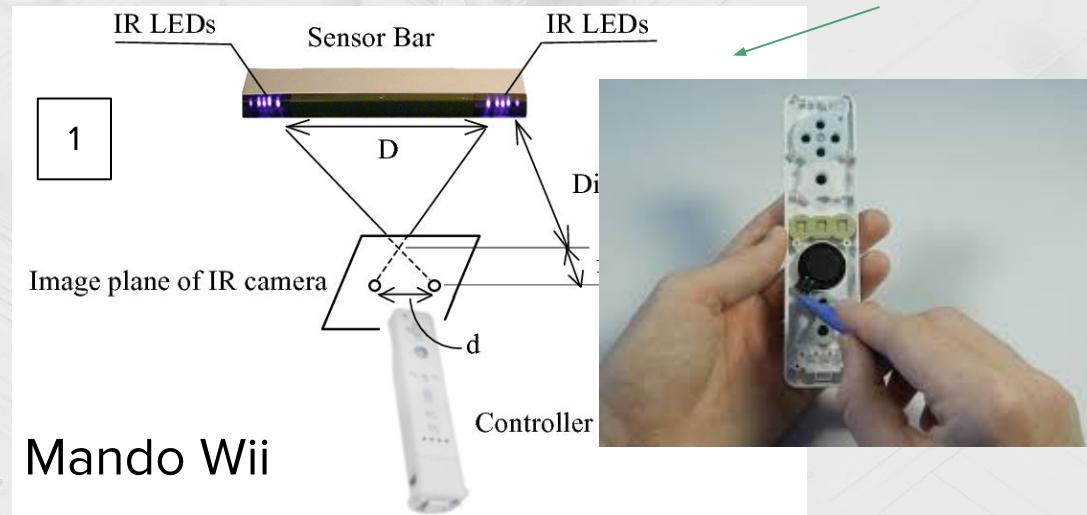
[f](#) [.](#) [p](#)



**It only spies
on the good bits...
we promise!**

Mando Wii, PSMove

- Sensores de movimiento
- Cámaras infrarrojas
- Micrófonos
- Bluetooth o WiFi
(Con vulnerabilidades)



Internet en las Consolas

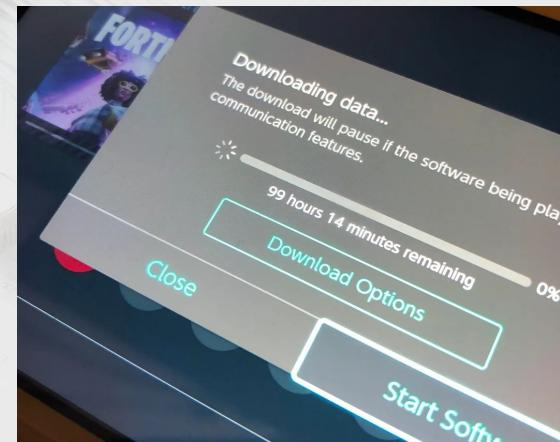
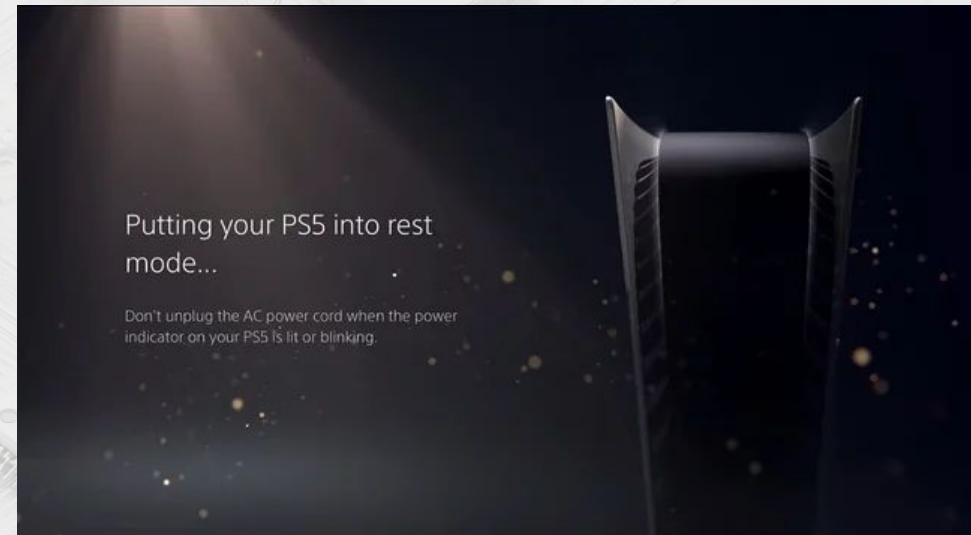
- Ethernet / WiFi

Requisito fundamental para:

- Jugar online
- Chats de grupo y llamadas
- Descargar juegos (No CDs)

Modos de espera:

- Conectadas 24/7
- Actualizaciones firmware, juegos...
- Te has conectado?
- Telemetría



Actualidad

-  Cámara (Algunas)
-  Micrófonos
-  Cuentas de usuario: Quién eres, a qué juegas, ... ➡ Servidores
-  Comportamiento: Juegos que te gustan, cuántos jugadores, con quién
-  Tarjetas de crédito (Necesarias) + Nombres completos + Direcciones
-  Netflix, Spotify, ...





Hablemos de negocios...

Brechas de seguridad (2011 - 2024)



En empresas de videojuegos:



PSN
2011

77 mill.



Blizzard
2012
14 mill.



Ubisoft
2014
58 mill.



Steam
2016
Millones



Epic Games
(Fortnite)
2018
Miles-Millones



Nintendo
2020
300.000



CD Project
Red
2021

No se hizo
público



Bandai
Namco
2022

No se hizo
público

Desde 2011:

- 149 millones cuentas aprox.
- Usuario-contraseña, emails, tarjetas, direcciones, ...
- No juegos gratis 😞



Vulnerabilidades para dummies

¿Qué es eso de “Vulnerabilidad”?

Ejemplo:

Error

Ejecuta lo que el usuario escriba

```
op = input("Ingresa un cálculo: ")
result = eval(op) # Ejecutamos la operación
print(f"El resultado es", result)
```

Lo que el programador espera:

```
Ingresa un cálculo: 2+2
El resultado es 4
```

Lo que hace el usuario:

```
Ingresa un cálculo: os.remove("System32")
:(
```

Qué se puede hacer...

- Shell reversa



```
op = input("Ingresa un cálculo: ")
result = eval(op) # Ejecutamos la operación
print(f"El resultado es", result)
```

```
Ingresa un cálculo: ssh-server listen
Connected!
```

- Activar cámaras



```
$ fswebcam 192.168.1.10:/foto.jpg
Picture taken! Sending...
```

- Grabar micrófonos



```
$ arecord -f cd 192.168.1.10:/microfono.wav
Grabando...
```

- Enviar datos a un servidor



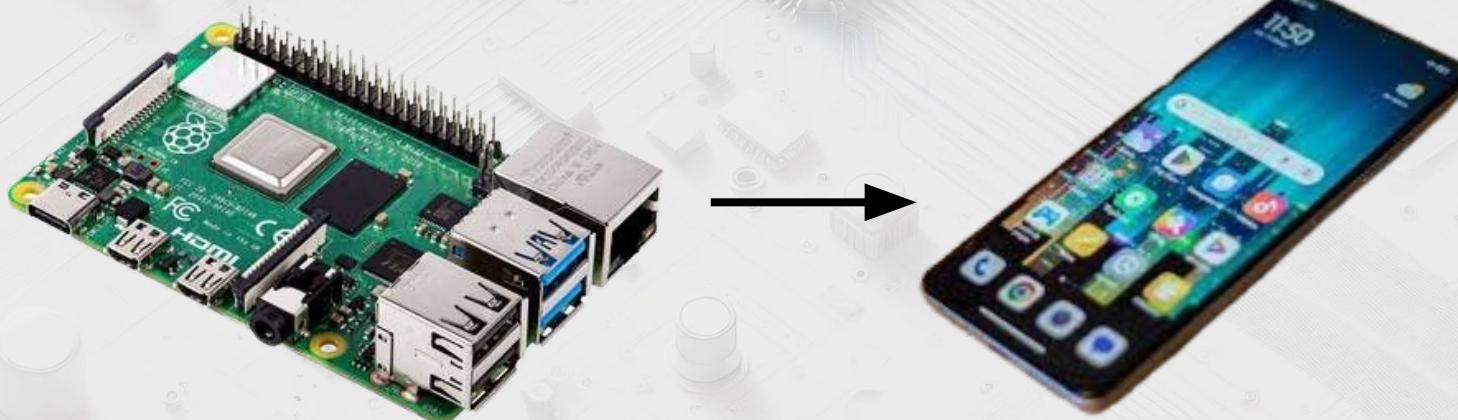
```
id > 192.168.1.10:/usuario.txt
:(
```

- ... El límite está en la imaginación



Consolas ➔ Sistemas en chip

- No tienes que conectar nada
- Simplemente funciona !!



El Código

- Lenguajes de programación
- Crean el sistema y los juegos

```
#include <iostream>
using namespace std;

int main() {
    cout << "Hello, World!" << endl;
    return 0;
}
```

C++

```
print("Hello, World!")
```

Python 

```
public class HelloWorld {
    public static void main(String[] args) {
        System.out.println("Hello, World!");
    }
}
```

Java 

Firmware
(Sistema operativo)

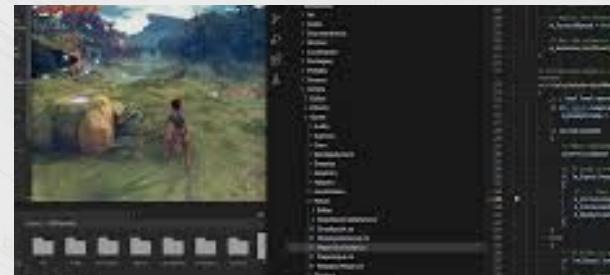
```
error = do_operation();
if (error) {
    dont();
}
return;
```

Linux 

```
1 import os
2 def Windows_Diagnostics():
3     print('Looking for problems')
4     waitTimer(20000ms)
5     print('Unable to fix the issue.')
6
```

Windows 

Juegos



Juegos 

Compilar

- Sistemas operativos ➔ C++

(La mayoría)

```
int a = 5;  
int b = 10;  
int sum = a + b;
```

Compilar



```
mov eax, 5  
mov ebx, 10  
add eax, ebx
```

Código C++

(El que entiende la gente normal)

Compilar



Consola

Código máquina

(El que entienden los dementes)

...

(Y las máquinas)

Ingeniería Inversa

```
55  
48 89 e5  
48 83 ec 10  
c7 45 fc 00 00 00 00  
b8 00 00 00 00  
83 f8 05  
7d 1f  
8b 14 85 00 00 00 00  
01 55 fc  
83 c0 01  
eb e6  
8b 75 fc  
48 8d 3d 00 00 00 00  
b8 00 00 00 00  
ff d0  
48 89 ec  
5d  
c3
```

??

Código máquina
(Binario)



```
push    rbp  
mov     rbp, rsp  
sub    rsp, 0x10  
mov    DWORD PTR [rbp-0x4], 0x0  
mov    eax, 0x0  
cmp    eax, 0x5  
jge    0x1f  
mov    edx, DWORD PTR [rax*4+0x0]  
add    DWORD PTR [rbp-0x4], edx  
add    eax, 0x1  
jmp    0xe6  
mov    esi, DWORD PTR [rbp-0x4]  
lea     rdi, [0x0]  
mov    eax, 0x0  
call   rax  
mov    rsp, rbp  
pop    rbp  
ret
```

???

Código máquina
(Ensamblador)

- No tenemos nombres de funciones o variables
- ¿Qué quería hacer el programador?

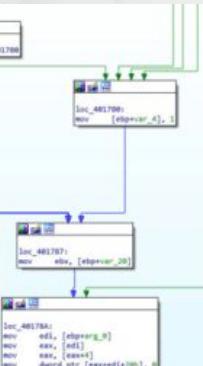
```
int sumar() {  
    int lista[5] = {1, 2, 3, 4, 5};  
    int suma = 0;  
  
    for(int i = 0; i < 5; ++i) {  
        suma += lista[i];  
    }  
    return suma;  
}
```

Código original

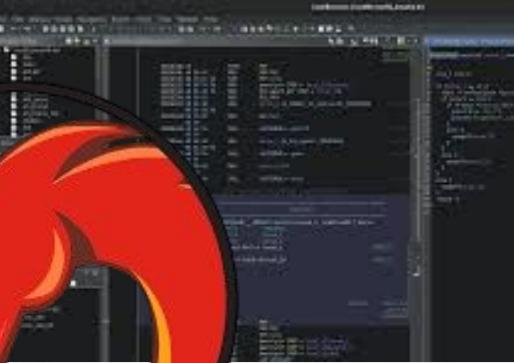
Herramientas para la Ingeniería Inversa



IDA



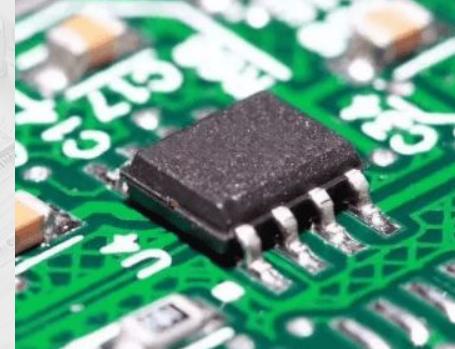
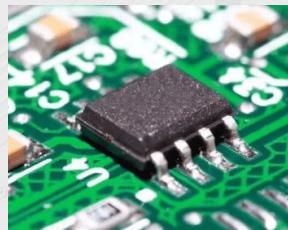
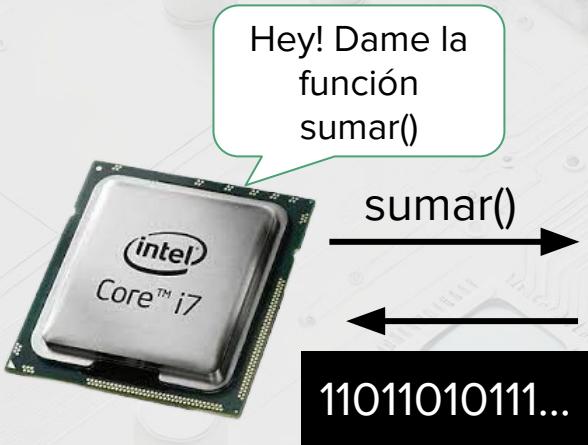
Ghidra



La memoria

El código:

- Se guarda en la memoria



Chip de memoria
soldado a la placa

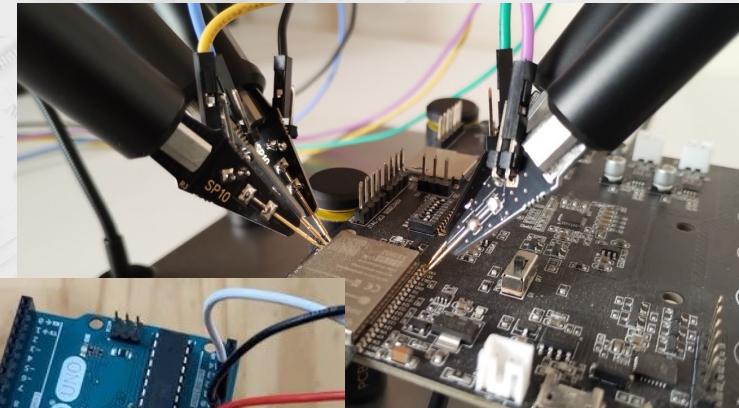
011110000010
010101010010
010100101011
01010001111

Código
(En binario)

Obteniendo el Código

Dos formas de extraer el firmware:

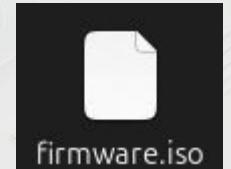
1. A lo bruto



2. Como unos profesionales



```
$ find C:/Windows/ > firmware.iso  
Dump finished.
```





Vamos a subir de nivel...

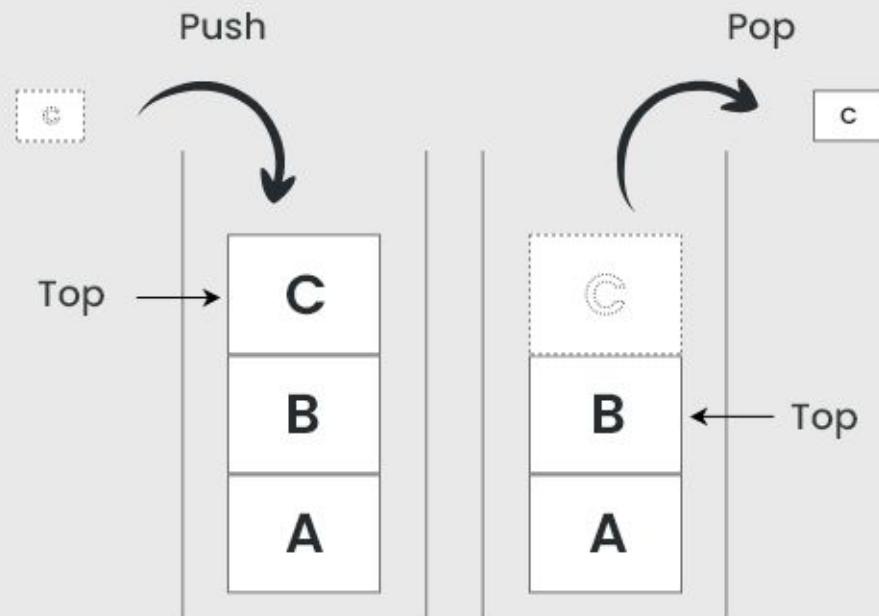
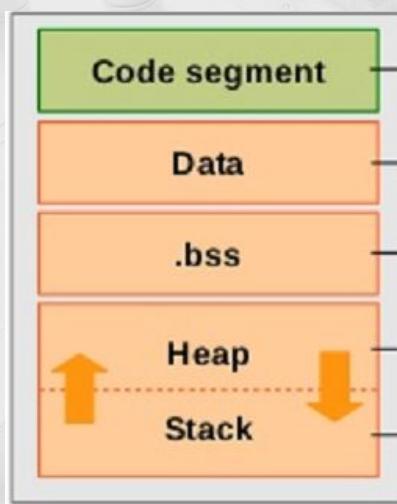
El Contador de Programa

- Determina el código que se está ejecutando
- Si lo escribimos, habremos ganado

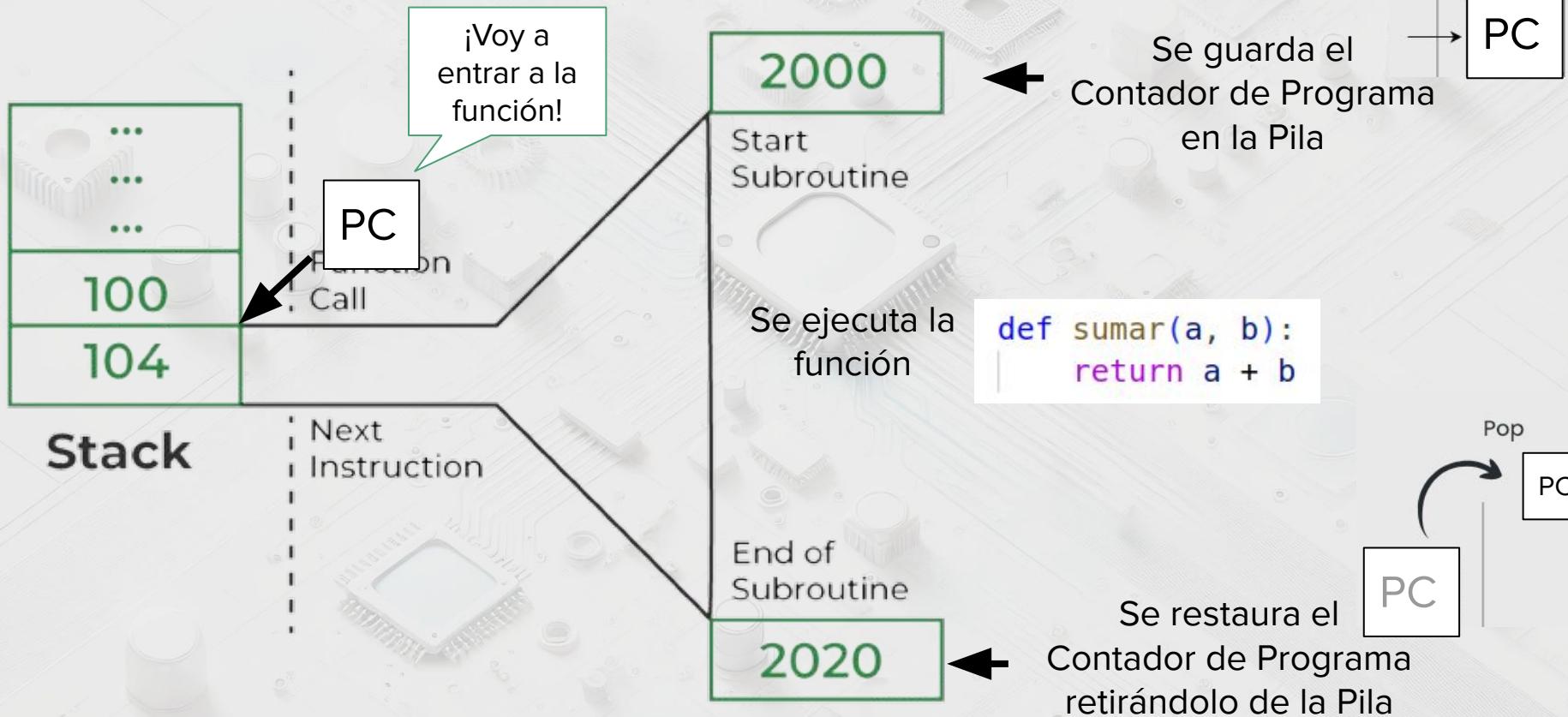


La Pila (o el Stack)

- Guarda Contadores de Programa
- Está al final de la memoria



La Pila (o el Stack)



Conclusión 1

Si logramos
escribir en la Pila



Conclusión

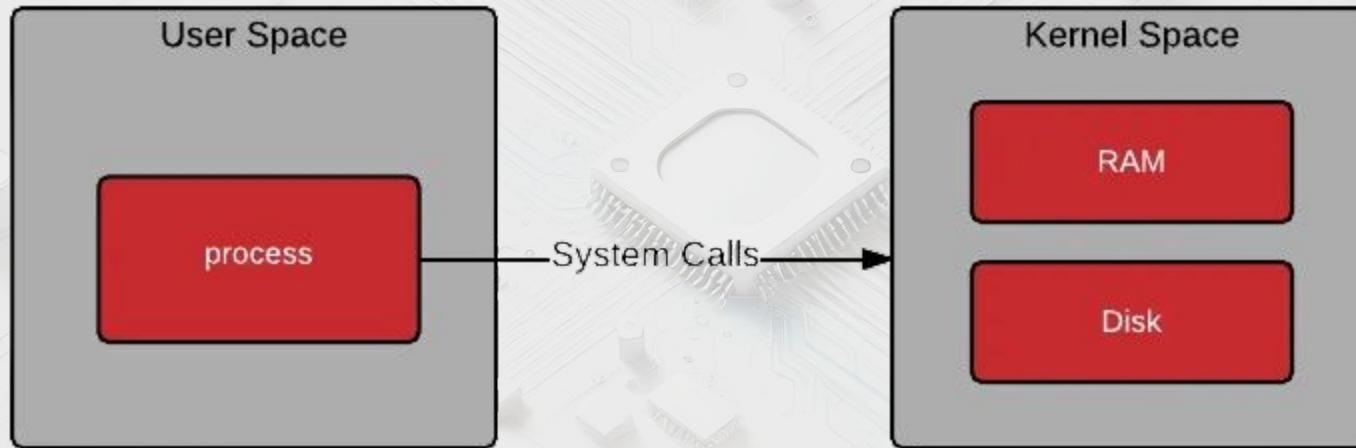
Escribimos el
Contador
de Programa



Tenemos el control
“Más o menos”



Espacio de Usuario, Espacio de Kernel



- Sin privilegios
 - Todo lo que puede ser peligroso
- Juegos, aplicaciones, navegador web...

- Todos los privilegios
 - Drivers, I/O, recursos, ...
- El Sistema Operativo

Conclusión 2

Conclusión

Si logramos
escribir en la Pila
del Usuario

Escribimos el
Contador
de Programa
del Usuario

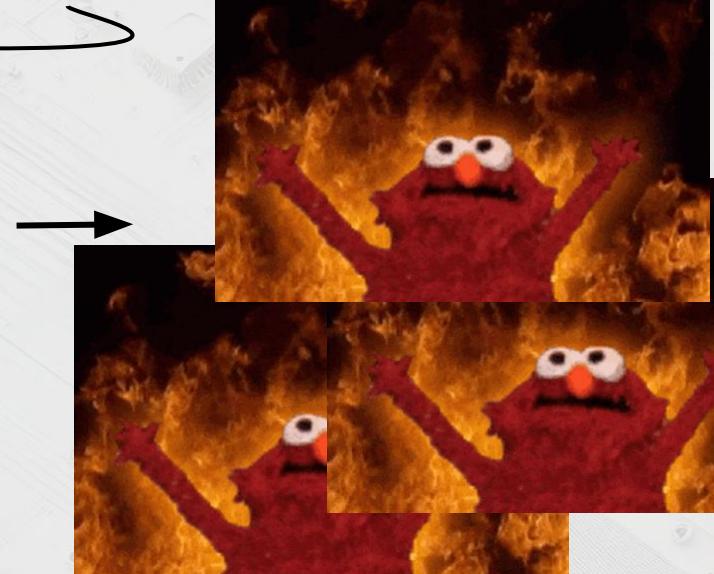
Tenemos control sobre el
espacio de Usuario



Control total sobre la
consola

Si logramos
escribir en la Pila
del Kernel

Escribimos el
Contador
de Programa
del Kernel





Fin de la clase.
Ahora vamos a lo interesante



3DS

Nintendo 3DS

El ejemplo perfecto:

- No implementa casi ninguna seguridad
- Portátil
- Tiene cámaras y micrófonos
- WiFi y comunicación con consolas cercanas



Te recompensaban por sacarla a la calle
(Contenido en juegos)

Nintendo 3DS

- ## - Dos procesadores →

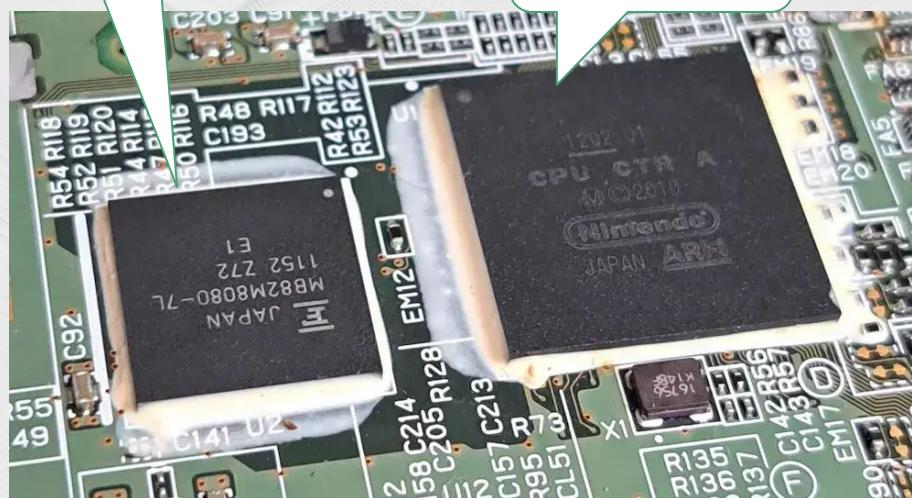
Objetivo:

Controlar el 2º procesador

¿Cómo?

Vale papá...

Niño no seas malo



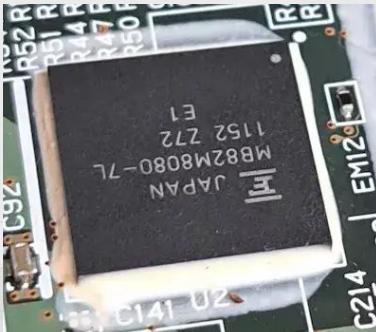
ARM11 (user)

- Juegos
 - Aplicaciones

ARM9 (kernel)

- Seguridad
 - Criptografía

Paso por paso



Paso 1:

- Ganar control sobre el espacio de usuario

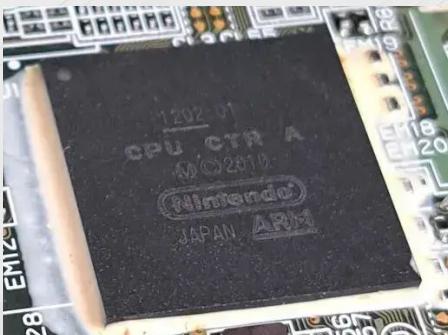
Problema:

Los programas solo utilizaban el procesador 1



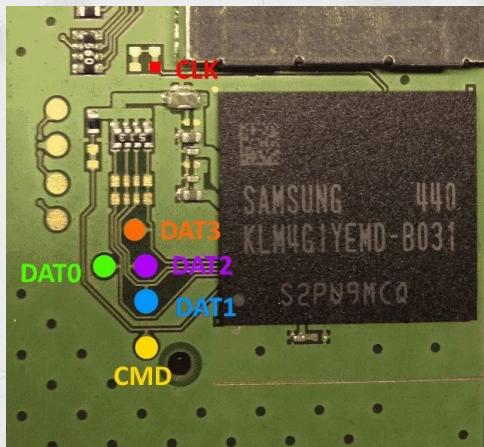
Paso 2:

- Romper el Kernel

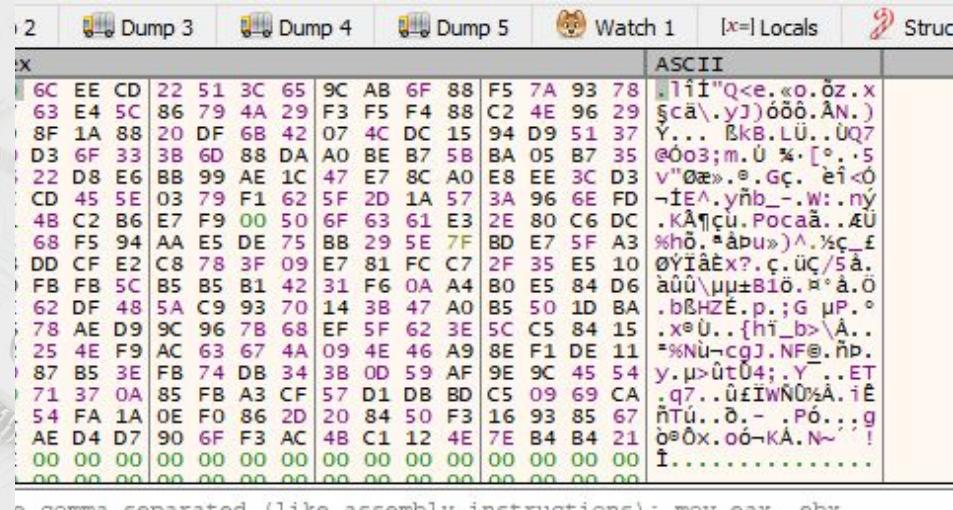


Encriptado de memoria

- Estaba toda encriptada... (SHA-1)

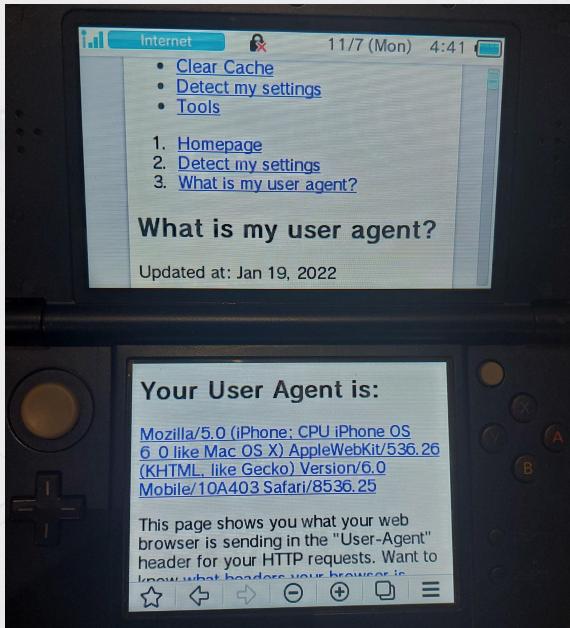


Memoria de la consola



- Memoria interna
 - Tarjeta SD
 - Archivos de guardado
 - ...

Paso 1. Espacio de Usuario



Tenía un navegador de internet:

- Basado en WebKit (iPhone, PlayStation, TVs, ...)
- Solo acceso al espacio de usuario
- Utiliza JavaScript → Podemos controlarlo

use-after-free

Corrupción de memoria

```
// Creamos la variable
let v = { programa: "print('Hello World')" };

// Liberamos la variable
v = null;

// Utilizamos la variable
console.log(v.programa);
```

Especificamos un programa

Quitamos la referencia
(Pero no lo borramos)

.....
.....print('Hello World').....
.....

Memoria

Utilizamos la variable

```
print('Hello World')
Hello World
```

El código se ejecuta !!!

Exploits de Juegos

- oot3dhax, smashbroshax, twilihax ...
- También vulneran el espacio de Usuario

Archivos de guardado, guardan:

- Nombre

... ¿Cómo un nombre puede vulnerar una consola?...



El Tamaño de las Partidas

Al abrir el juego:

- Se carga la partida en memoria
 - ¿Y si la partida es más grande que la memoria?

```
void* partida = leerPartida();
void* buffer = malloc(0x100);

memcpy(buffer, partida);
```

En realidad es un programa

No se comprueba que la partida quepa en el buffer !!!

buffer overflow

El programa es más grande que la memoria

```
void* partida = leerPartida();
void* buffer = malloc(0x100);
memcpy(buffer, partida);
```

La partida es un programa

```
0x0C0: 00 00 00 00 00 | .....  
0x0D0: 00 00 00 00 00 | .....  
0x0E0: 00 00 00 00 00 | .....  
0x0F0: 00 00 00 00 00 | .....  
0x100: 32 BD 12 23 45 | Otros datos  
0x110: 43 21 09 87 65 | del programa  
0x120: A5 2B 3C 4D 5E |
```

0x0C0:	FF	FF	FF	FF	FF		AAAAAAAAAA
0x0D0:	FF	FF	FF	FF	FF		AAAAAAAAAA
0x0E0:	FF	FF	FF	FF	FF		AAAAAAAAAA
0x0F0:	FF	FF	FF	FF	FF		AAAAAAAAAA
0x100:	FF	FF	FF	FF	FF		AAAAAAAAAA
0x110:	FF	FF	FF	FF	FF		AAAAAAAAAA
0x120:	FF	FF	FF	FF	FF		AAAAAAAAAA



Y si es un Juego Online?

ENLBufferPwn:

- Juegos: Mario Kart 7, Animal Crossing, ...
- Buffer overflow remoto

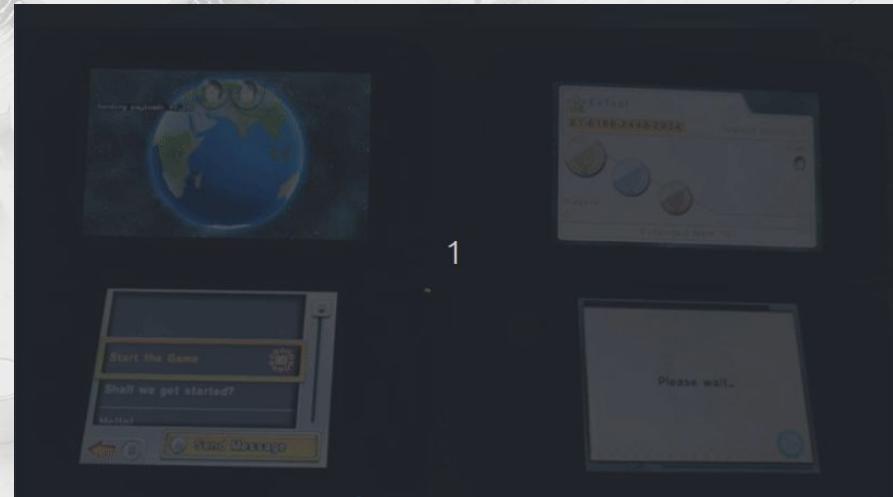
ENLBufferPwn (CVE-2022-47949)



**ENL
BUFFERPWN**

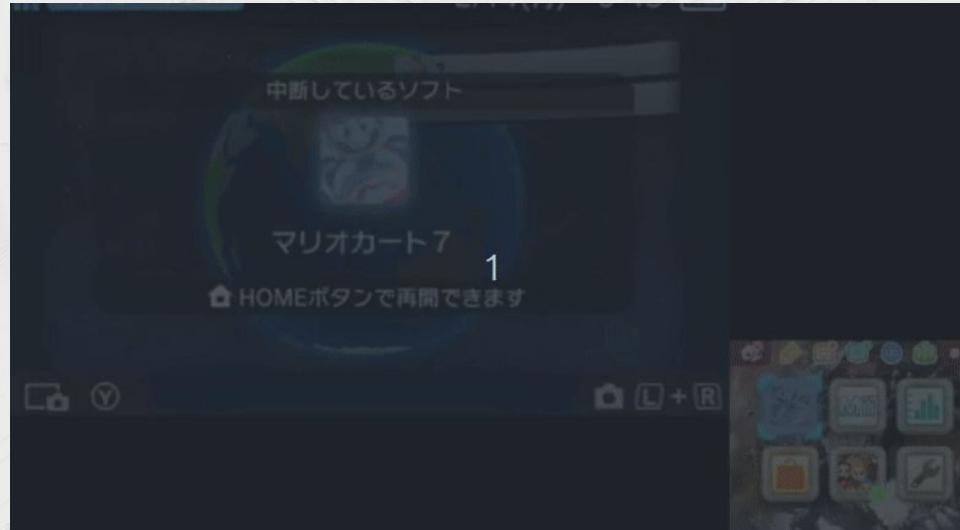
CVE:	CVE-2022-47949
CVSS v3.1:	9.8/10 (Critical)

Podías vulnerar otras consolas remotamente



ENLBufferPwn

Reportes desde 2021...



... ¿Y si lo usaran
para el mal? ...

Hackers ya ejecutaban código en partidas online
En este caso: Algo vanal. Solo entrar y salir del juego

SwapNoteRCE

Ni siquiera hace falta estar en una partida online...

[3DS][StreetPass] Heap Overflow in Swapnote parser leads to userland
StreetPass RCE

```
u32 offset_0 = *(u32*)(TLRF_buffer + 0x6DC);
u32 size_0 = *(u32*)(TLRF_buffer + 0x70C);
memcpy(heap_buffer_0, TLRF_buffer + offset_0, size_0);
```



Controlado por la consola
que manda el mensaje
Buffer overflow remoto

- Se podía ejecutar al recibir un mensaje de otra consola



(En la calle por ejemplo)



Wii

Wii

- Similar a la 3DS → Dos procesadores



Seguridad:

- Cadena de confianza
- Módulo OTP (One-Time-Programmable)

Cadena de Confianza

Se enciende la
Start consola

ARM

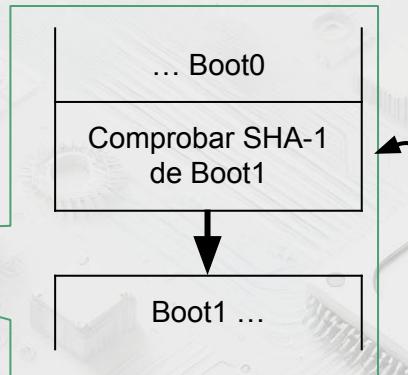
boot0

boot1

boot2

SysMenu IOS

Game/Title IOS



Clave pública



Clave privada

- Cada fase del arranque comprueba a la siguiente
- ¿Por qué no podemos firmarlas nosotros? → Algoritmo RSA

Firma la
cadena

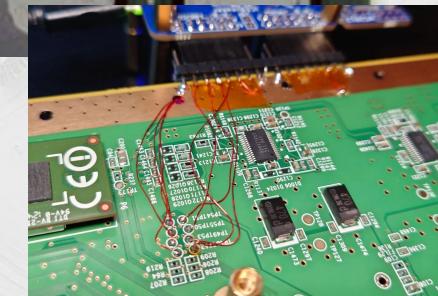
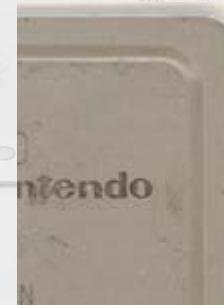


- 40 caracteres
- 2^{160} posibles combinaciones

Módulo OTP (One-Time-Programmable)

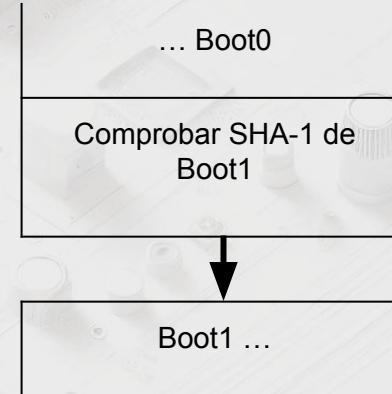
Memoria de 1 sola escritura:

- Solo lectura
- No puedes modificarlo
- Donde se almacenan las claves públicas

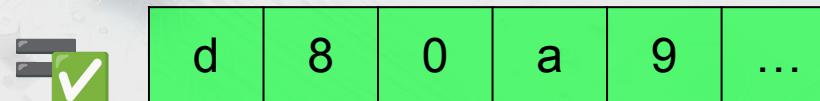
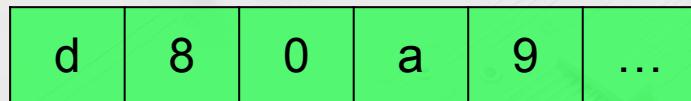


Explotando la Cadena de Confianza

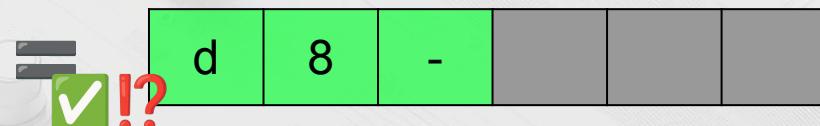
- Error en el código de verificación
- Ejemplo:



Comprobación 1



Comprobación 2



Fin de la
cadena

Explotando el Algoritmo RSA

Tenemos que encontrar una clave:

- Con al menos 1 dígito igual a la clave real
- **✗** No valen cadenas vacías

Clave de boot0:
(Fase 1)

a	9	5	...
---	---	---	-----



$2^1 = 256$ posibles combinaciones
Menos de 1 segundo de cálculo...

Clave calculada:

a	-		
---	---	--	--



Tablero de mensajes

Aplicación de mensajería

- Enviar texto de una consola a otra

¿Cómo podemos utilizar esto?



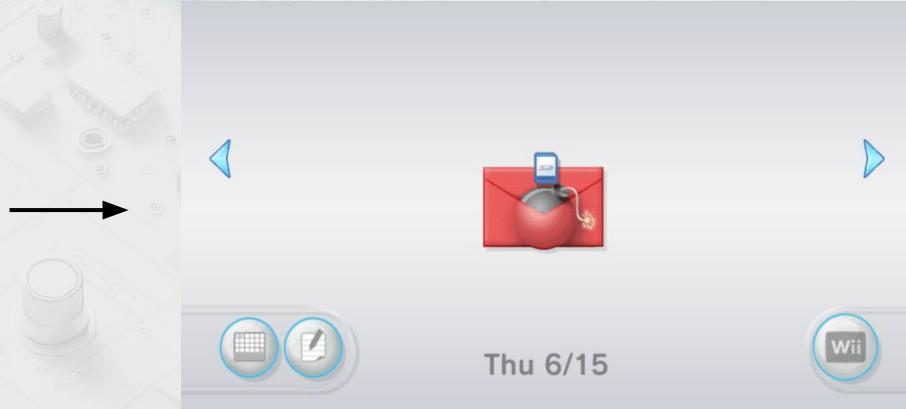
LetterBomb

Buffer overflow
en las cartas

→ Solo tenías que indicar
la dirección MAC



El exploit se activaba al abrirlo

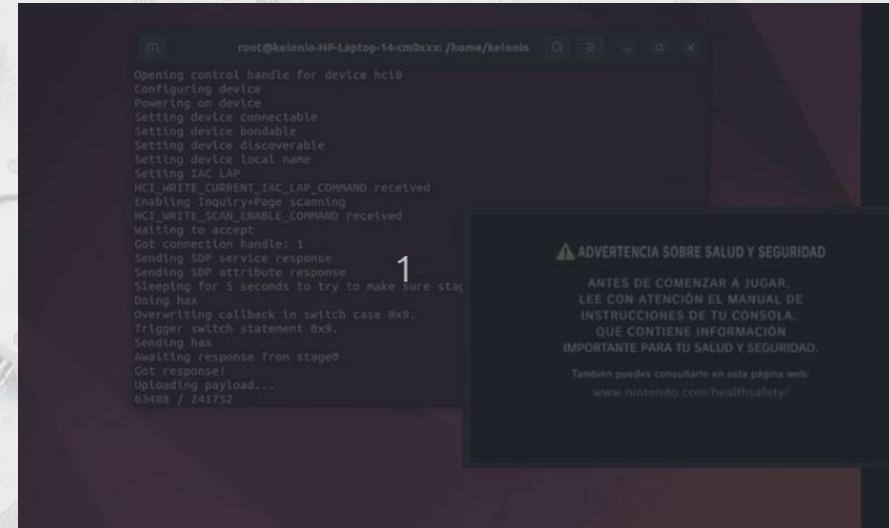


Bluebomb

- ¿Y si no hiciera falta abrir la carta?
- Exploit en el Módulo de Bluetooth

Paso a paso:

1. Se conecta un ordenador
(Simulando al mando)
2. Mandamos un programa gigante



```
root@kelonio-HP-Laptop-14-cm0xxx: /home/kelonio
Opening control handle for device hc0
Configuring device
Powering on device
Setting device connectable
Setting device bondable
Setting device discoverable
Setting device local name
Setting IAC LAP
HCI_WRITE_CURRENT_IAC_LAP_COMMAND received
Enabling InquiryPage scanning
HCI_WRITE_SCAN_ENABLE_COMMAND received
Waiting to accept
Got connection handle: 1
Sending SDP service response
Sending SDP attribute response
Sleeping for 5 seconds to try to make sure stats
Doing hax
Overwriting callback in switch case 0x9.
Trigger switch statement 0x9.
Sending hax
Awaiting response from stage0
Got response
Uploading payload...
03408 / 241752
```

ANTES DE COMENZAR A JUGAR,
LEE CON ATENCIÓN EL MANUAL DE
INSTRUCCIONES DE TU CONSOLA,
QUE CONTIENE INFORMACIÓN
IMPORTANTE PARA TU SALUD Y SEGURIDAD.
También puedes consultarla en esta página web:
www.nintendo.com/healthsafety/

La consola lo ejecuta, sin
interacción del usuario

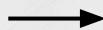
Buffer overflow
remoto

Bluebomb

Presente en más dispositivos

- No era un error de la Wii

Causante



Módulo Bluetooth
Broadcom BCM2045

Móviles



Varios teléfonos Samsung

Coches



BMW Serie 3



Volkswagen Golf

Disclaimer !!



¿ Wii U ?



PS4

PlayStation 4

Casi como un PC:

- 1 procesador
- Gráfica AMD Radeon

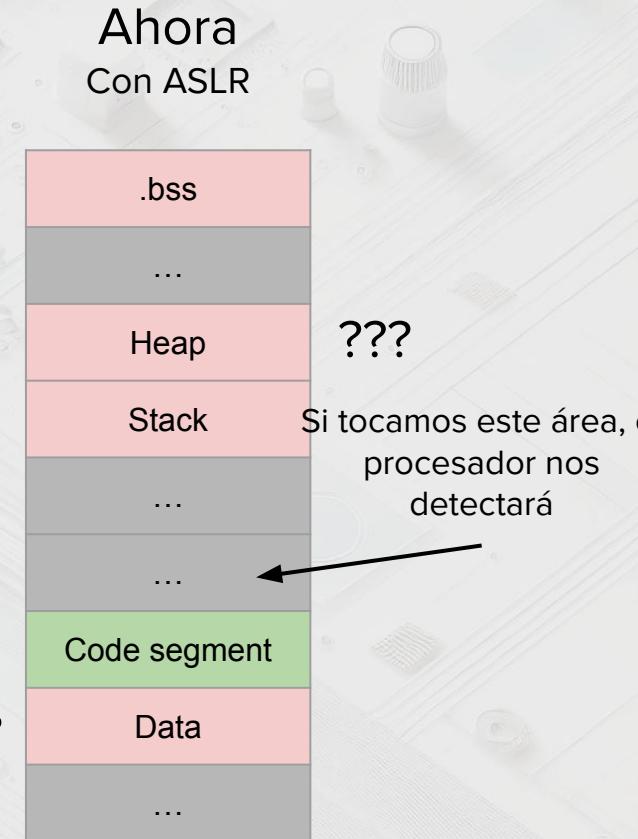
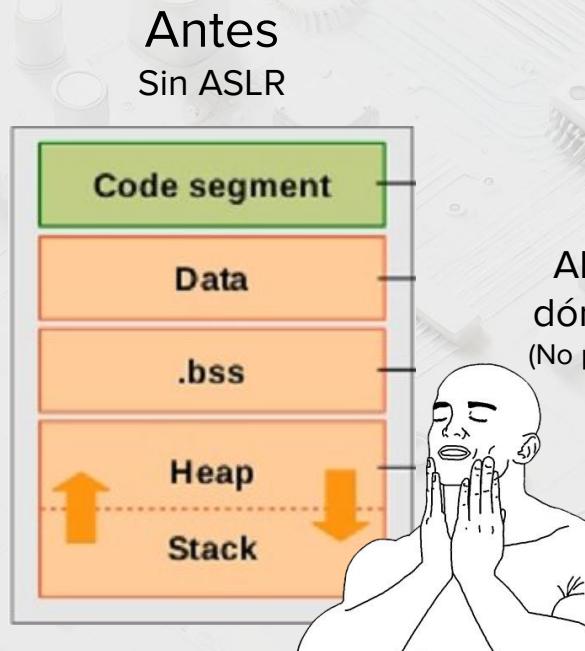
Seguridad:

- ASLR
- Hypervisor
- Fusibles



ASLR (Address Space Layout Randomization)

Separar la memoria aleatoriamente

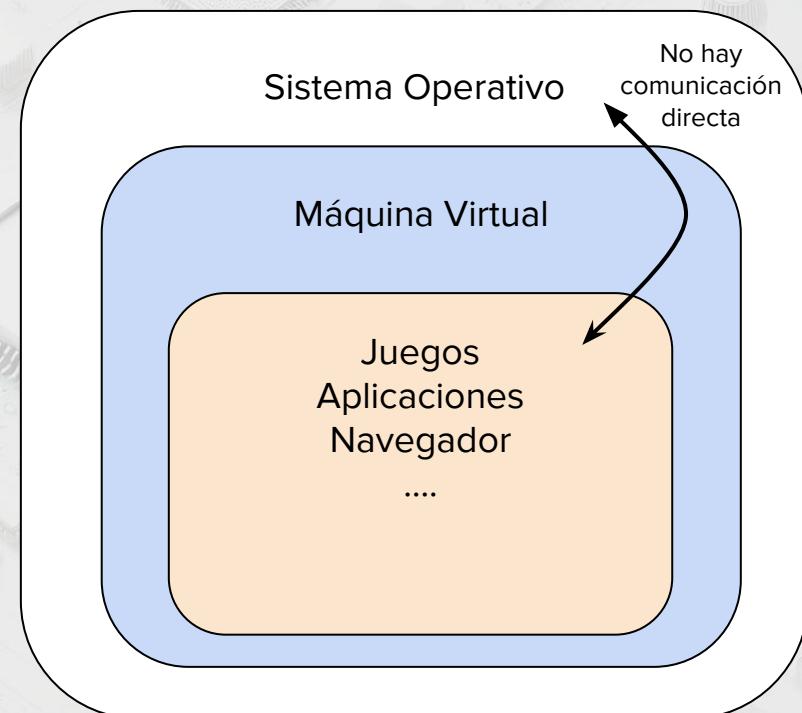


Hypervisor

Una máquina virtual para:

- Juegos
- Aplicaciones
- Navegador Web
- ...

En esencia, todo lo peligroso



Fusibles

Fusibles microscópicos

Cada vez que actualizamos → Se quema uno

Utilidad:

- Prevenir desactualizaciones
- ... Para volver a versiones con vulnerabilidades

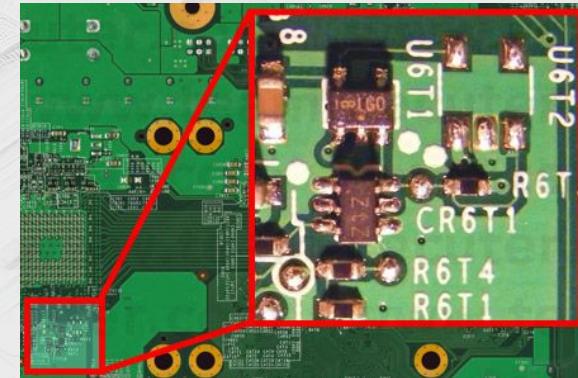
Actualización con 9
fusibles quemados



El usuario tiene 11
quemados



Ha desactualizado !!
Apagar.



FreeBSD

Sistema operativo de PS4 → Basado en FreeBSD
(Kernel)

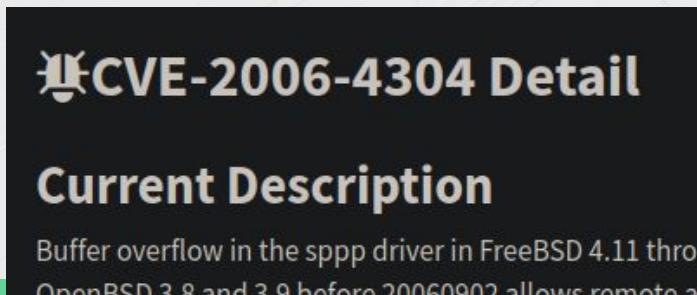
FreeBSD 9.0:

- Código abierto (Similar a Linux)
 - Vulnerabilidades conocidas (Desde 2012)
 - Vamos a ver unas cuantas...

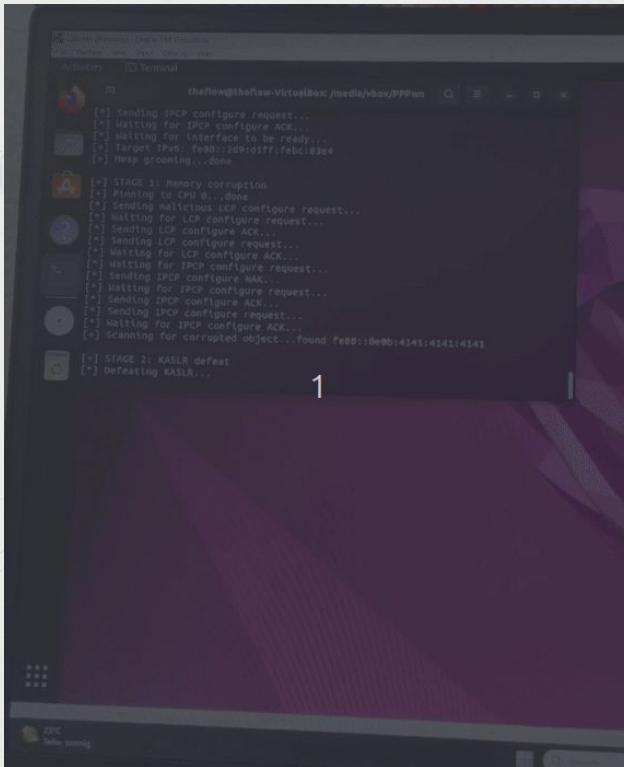


PPPwn RCE

- buffer overflow en el Driver de Ethernet
 - Driver de Ethernet → Dentro del espacio de Kernel
(Control sobre el Kernel)
 - Permite ejecutar código remotamente
 - Público desde 2006 !!

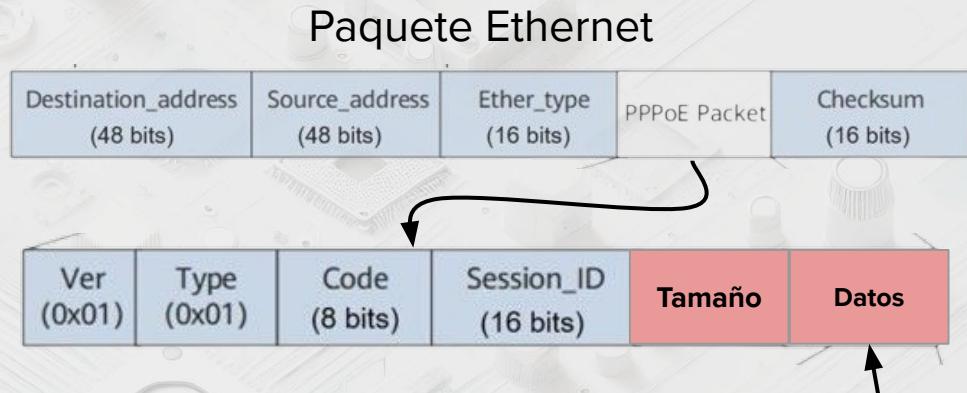


PPPwn RCE



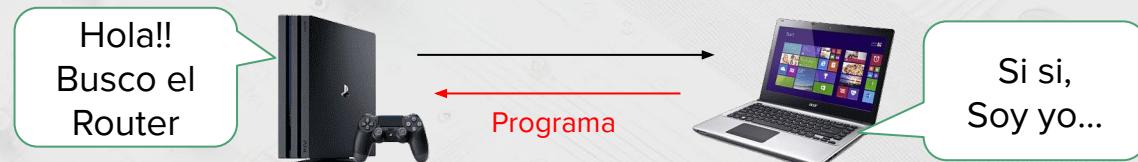
```
theFlow@theFlow-VirtualBox:~/media/rbx/PPPwn
[+] Sending IPCP configure request...
[+] Waiting for IPCP configure ACK...
[+] Waiting for interface to be ready...
[+] Target IPv6: fe00::1:2:1:1:febc:83e4
[+] Head grooming...done

[+] STAGE 1: Memory corruption
PINNING to CPU 0...done
[+] Sending LCP configure request...
[+] Waiting for LCP configure request...
[+] Sending LCP configure ACK...
[+] Waiting for LCP configure ACK...
[+] Sending LCP configure request...
[+] Waiting for LCP configure ACK...
[+] Sending LCP configure request...
[+] Waiting for LCP configure ACK...
[+] Sending LCP configure request...
[+] Waiting for LCP configure ACK...
[+] Sending IPCP configure request...
[+] Waiting for IPCP configure ACK...
[+] Scanning for corrupted object...found fe00::1:2:1:1:febc:83e4
[+] STAGE 2: KASLR defeat
[+] Defeating KASLR...
1
```



buffer overflow:

1. La consola pregunta por routers
2. Nuestro ordenador responde, mandando un paquete con el programa dentro del campo “contraseña”



Conclusión

- No hace falta un exploit de Usuario
- Podemos explotar remotamente el Kernel



Vuelvo a hacer la pregunta:

¿Y si se usara para el mal?...



Xbox Series

Xbox Series

- No se puede hackear
- Pero a nadie le importa !!



PS5

Xbox Series

Tiene matices:

- Todos los dispositivos se pueden hackear
- Problema: Nadie estaba interesado



... ¿Por qué? ...

Analicemos a los Hackers

Qué no les interesa:

-  Piratear juegos

Qué les interesa

-  Emuladores
-  Linux
-  Aplicaciones hechas por usuarios

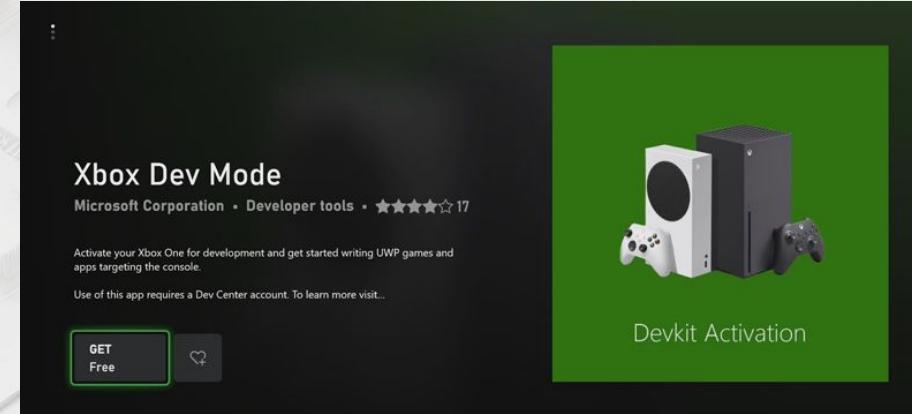


... Y Microsoft se lo dio

Dev Mode

Por 20\$ al mes permitía:

- Activar el modo Desarrollador
- Ejecutar tus propias aplicaciones (Emuladores, reproductores, ...)



Hasta que...

**MICROSOFT COMENZÓ A BLOQUEAR
EMULADORES EN XBOX SERIES X|S**

Collateral Damage

Tan solo unos meses más tarde

Game Script:

- Entorno de programación (Tipo Python) → Ejecución de código de Usuario
- Solo nos hace falta escalar privilegios !!!

```
MasterControl:AddToPlayerMovement(Vector3.new(0, 0,
CurrentThrottle = (inputState == Enum.UserInputStat
MasterControl:AddToPlayerMovement(Vector3.new(0, 0,
Accelerating = not (inputState == Enum.UserInputSta
if (inputState == Enum.UserInputState.End) and Deco
    CurrentThrottle = 1
    MasterControl:AddToPlayerMovement(Vector3.new(0
end
end

local function onThrottleDeccel(actionName, inputState,
    MasterControl:AddToPlayerMovement(Vector3.new(0, 0,
```

race-condition

```
def sistema():
    while True:
        if (objeto.existe):
            eliminar(objeto)

def juego():
    while True:
        objeto = crearObjeto()
        print('Hello World')
    
```

Nosotros:

- Escribimos el programa repetidamente

El sistema:

- Intenta borrar los objetos

Tarde o temprano, se equivocará:

- Al leer el objeto, indirectamente ejecutaría las instrucciones que indicamos dentro

Conclusión

- Exploits y frameworks comenzando su desarrollo

solstice

A multi-stage PE loader for [@carrot_c4k3's CollateralDamage](#)
Xbox One exploit.

- No es que no se pudiera ➔ Es que no se había intentado (o no era público)
- Ahora sí, pasemos a la siguiente...



PS5

PlayStation 5

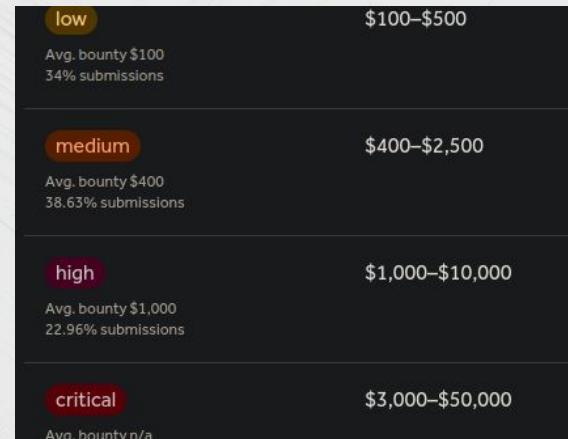
La más moderna → En el punto de mira de los hackers



Sony se sacó programa Bug Bounty → Hasta 50.000€ recompensa

Todas las medidas de seguridad anteriores + Algunas más:

- ASan
- XOM
- Kernel dentro de la máquina virtual



ASan (Address Sanitization)

Se comprueban todos los accesos a memoria

Si hay una dirección protegida:

- Se apaga la consola

Direcciones protegidas:

- Variables liberadas → **use-after-free**
- Accesos a la pila → **buffer overflows**

Antes
Sin ASan

```
*variable = 0x1000  
leer(variable)
```

Ahora
Con ASan

```
*variable = 0x1000  
  
if (memoria protegida)  
    error()  
else  
    variable = leer()
```

XOM (eXecute Only Memory)

Sin XOM

Las páginas de memoria:

- Tienen los atributos RX
(Se puede leer y ejecutar)

Podemos leer el
código de la consola

Buscar
vulnerabilidades

Con XOM:

Memoria de sólo ejecución

- Sólo atributo X → No podemos leer el
código



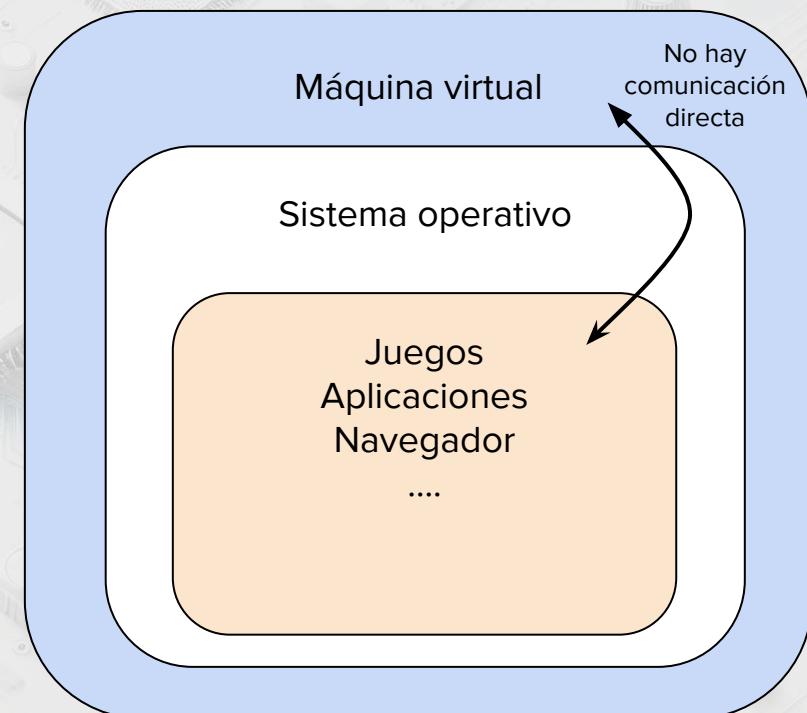
Kernel dentro del Hypervisor

El Kernel también se ejecuta dentro de la máquina virtual

- Vigila al Kernel constantemente
- El Kernel hace las operaciones a través de llamadas a la máquina virtual

0	GET_MESSAGE_CONF
1	GET_MESSAGE_COUNT
2	START_LOADING_SELF
3	FINISH_LOADING_SELF
4	SET_CPUID_PS4
5	SET_CPUID_PPP

(Muy pocas llamadas)



Primer exploit: bd-jb

Los lectores de CDs pueden leer Java:

- Menús interactivos en películas



Blu-ray de Avengers: Endgame

Error en la máquina virtual de Java

- Podemos modificar un archivo de configuración → Inyectar código Java
- El Kernel lee el archivo y ejecuta el código → **Acceso al Kernel !!**

Injectamos
nuestro código en
la configuración

```
ObjectOutputStream config =  
    new ObjectOutputStream("user.config");  
config.writeObject("print('Hello World')");
```

```
ObjectOutputStream config =  
    new ObjectOutputStream("user.config");  
Object codigo = (Object)config.readObject();  
Nuestro código se ejecuta !!
```

Bypervisor

Tenemos que ganar control de la máquina virtual

Llamadas al sistema:

Retrocompatibilidad con PS4

- Elegir en qué núcleo se pondrá nuestro código

2	START_LOADING_SELF
3	FINISH_LOADING_SELF
4	SET_CPUID_PS4
5	SET_CPUID_PRR

Hypervisor
comprobará si
podemos

Hacemos repetidas
llamada para distintos
núcleos
(race-condition)

Nos colocará en el
mismo núcleo que
la máquina virtual

Después

Hemos conseguido ejecución dentro de la máquina virtual

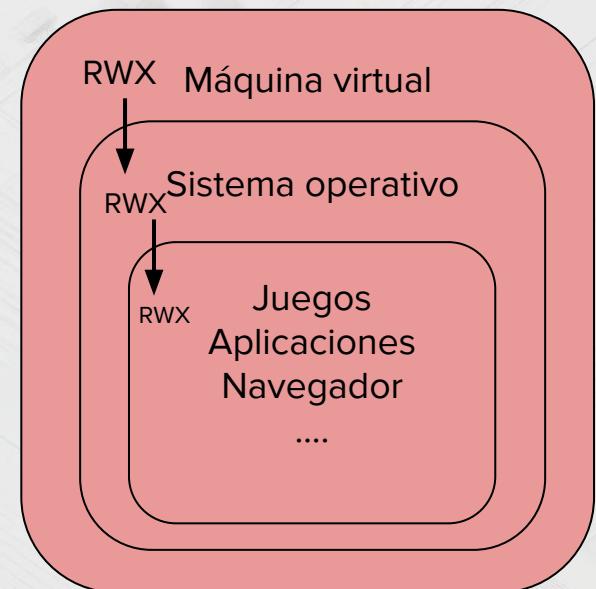
Desactivamos el XOM → Permisos RWX

Leer, escribir y ejecutar

Hemos ganado



... ¿Y si lo hacemos
remotamente? ...



CVE-2020-7457

PS5 → También basada en FreeBSD (11.0)

Exploit de FreeBSD en el driver IPv6



Driver IPv6 está **dentro del Kernel**

- Cargamos una web que mande muchas peticiones IPv6
- Cada petición es un puntero → Tarde o temprano fallará y nos dará un puntero con permisos sobre el driver IPV6 (race-condition)
- Control sobre el Kernel !!

Contra: El usuario tiene que entrar a la Web

... ¿Podemos mejorarlo?...



PPPwn RCE 2

Exploit PPPwn de PS4 → También disponible en PS5

 **CVE-2006-4304**

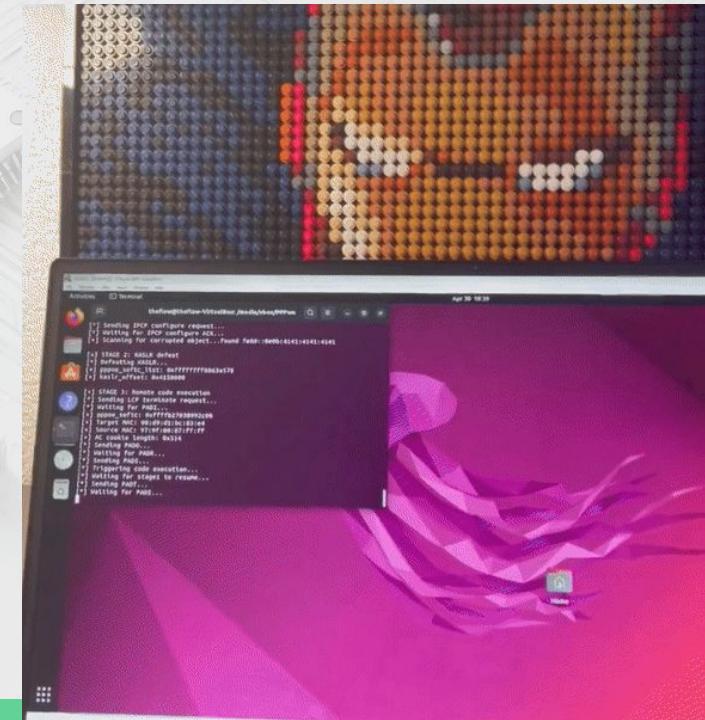
- Ejecución remota de código en PS5
- Exactamente igual que en PS4

Y si lo juntamos todo...

PPPwn +
Bypervisor



Acceso a toda la
consola
remotamente



Recapitulando...

Exploits

- No son difíciles de hacer
- Todo es público

Cualquiera puede modificarlo a su gusto

Hackers los desarrollan por:

- Diversión
- Ejecutar sus propias aplicaciones
- ... ¿Pero se pueden usar para el mal? ... Vamos a intentar demostrarlo



Conociendo a Nuestra Víctima

No he hablado de una consola en particular:

- Popular (También entre los niños)
- Conexión 24h a internet
- Información sensible: Cuentas, contraseñas, ...



¡Es perfecta!
Vamos a ver por qué...



Switch

Nintendo Switch

- Portátil
- Procesador Nvidia Tegra X1

Seguridad:

- ASLR, Cadena de confianza, VM...
- Fusibles
- Eliminar el navegador (🚫 WebKit)

Lo utilizan teléfonos
Ejemplo: Galaxy A53



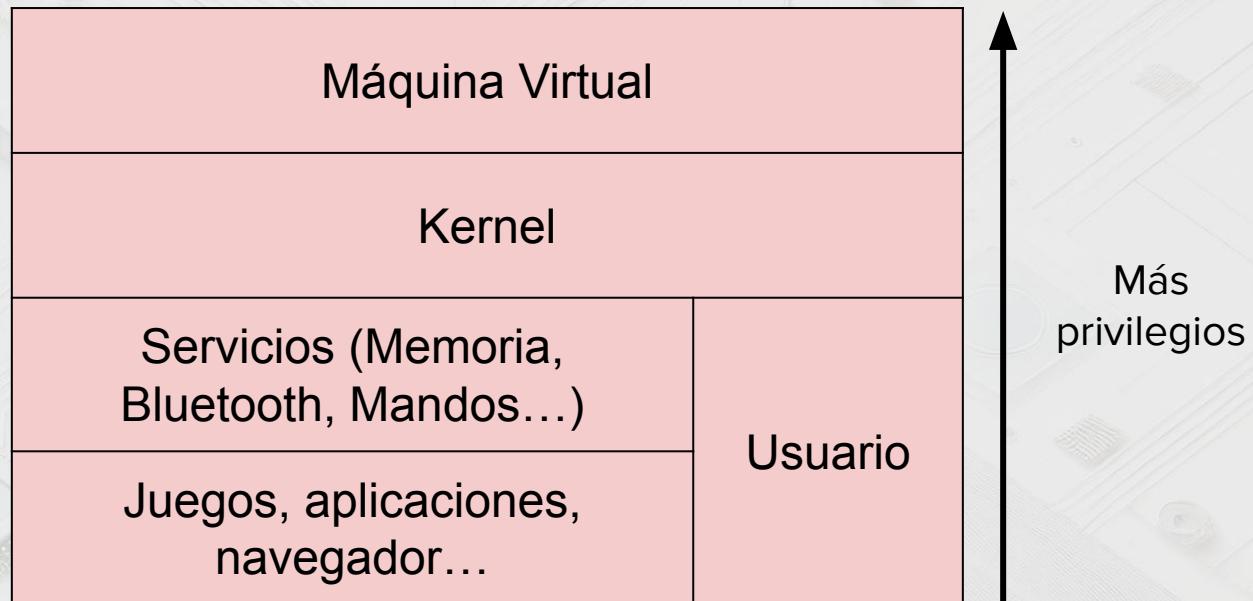
Manual de 3000 páginas de cómo
programar en el (Público)



Pero ningún sistema es perfecto...

Conociendo al Objetivo

Modelo de seguridad de la Nintendo Switch:



Vamos a empezar
por aquí



Accediendo al Navegador

Realmente quitaron el navegador...? → **No**
Solo lo ocultaron

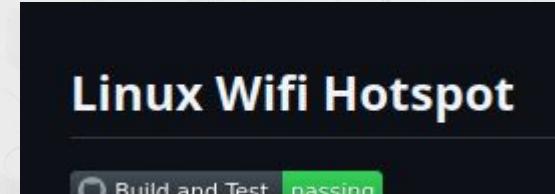
Accesible para Hotspots → Cafeterías, hoteles, ...

Normalmente HTTP
(Sin HTTPS) → Podemos hacer **DNS Poisioning** y mostrar nuestra propia Web



Exploit del WebKit

- Simulamos que nuestro ordenador es un Hotspot



Vulnerabilidad PEGASUS:

- Exploit del navegador web
- Presente también en dispositivos iOS (iPhone 5, 6, ...)
- use-after-free en JavaScript

Curiosidad:

```
let lista = [
  null,
  ...
  "print('Hello, World!')"
]

let programa = array[9]

lista = null;

console.log(programa)
```

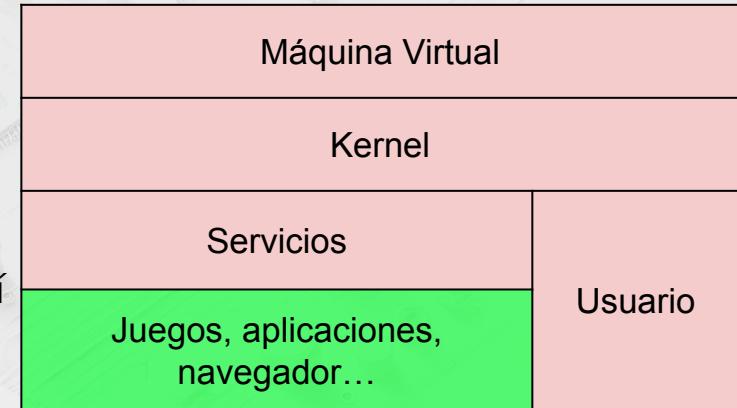
- Guardamos el código en un array
- Quitamos la referencia al array
- El código NO se ha borrado. Se ejecuta

Exploit de los Servicios

Servicios:

- Mapa de Memoria
- Dispositivos (Mandos, WiFi, ...)

Estamos aquí



Se tienen que inicializar

```
smInitialize(sm_handle);  
smGetService(sm_handle, "bluetooth");
```

Manda nuestros privilegios

- ¿Y si no?

Control total sobre los servicios

```
sm_handle = null;  
smGetService(sm_handle, "bluetooth");
```

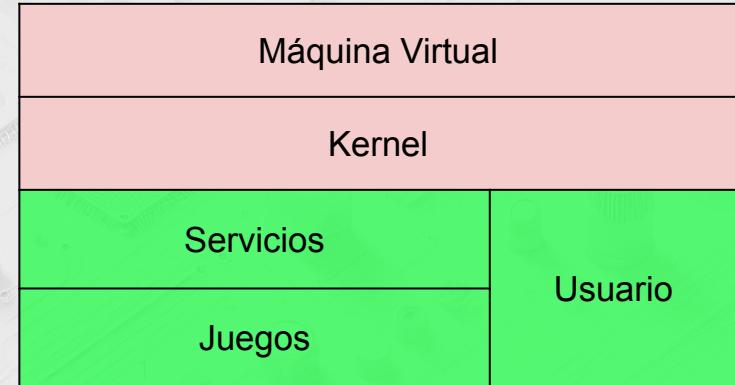
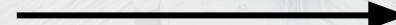
Privilegios = 0 (Máximos)

Exploit en el Kernel

Tenemos acceso al servicio de mapa de memoria

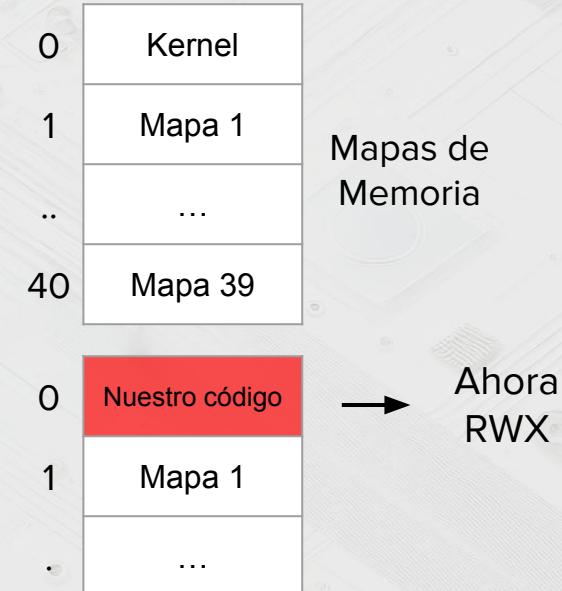
Los mapas se almacenan en una lista:

- Kernel → 1er elemento
- Máximo 40 elementos



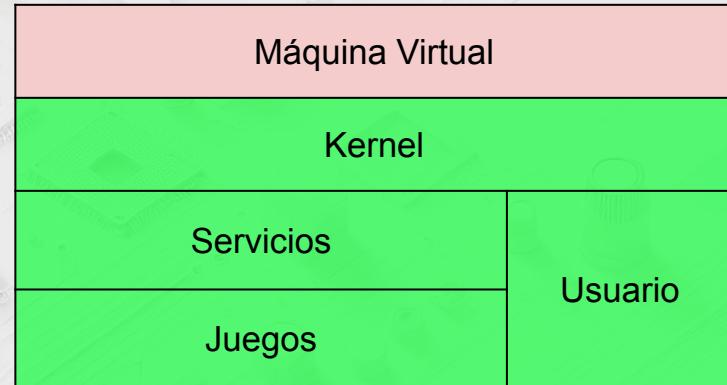
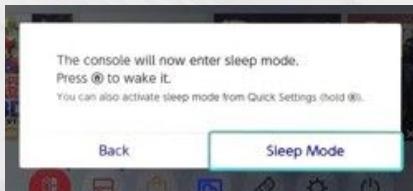
Y si llegamos a 40? → Volvemos al primero

- Podemos escribir encima del Kernel



Exploit de la Máquina Virtual

Modo de Espera:



- Guarda el estado en la memoria y apaga el procesador

Con acceso al Kernel:

- Podemos sobreescribir el código de la máquina virtual
 - Al despertarse se ejecutará nuestro código

```
0000000000 01 bc 67 db 99 1e 24 e0 99 e3 e3 16 e1 e
000000010 22 70 24 79 0b 66 9b 90 fb 19 62 75 82 3
000000020 44 6c 71 c6 61 67 a0 17 72 06 a6 68 a1 6
000000030 8c 44 7d c2 98 10 40 4b 7d ca 4c 26 06 e
000000040 57 b1 6c 98 sc9 18 34 e1 d0 b1 e4 4c ed b
000000050 23 20 4d 36 17 6c 9d dc b2 09 6e 38 db 6
000000060 22 0f 4c aa 66 36 c6 14 7f 0d a6 76 ad 7
000000070 df 59 56 dd 9e 1a 42 45 28 d4 76 3e 65 8
000000080 44 bb 6d dd 93 4b 1f da cc b6 fe 16 bd d
```

ENLBufferPwn

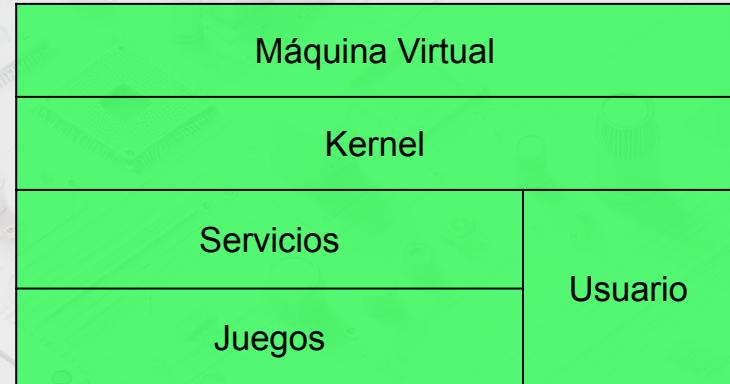
Vamos a hacerlo remoto

El mismo que el de la 3DS

Podemos encadenar exploits
hasta ganar control en la
máquina virtual



Empezamos
desde aquí



- Mario Kart 8 Deluxe (fixed in v2.1.0)
- Animal Crossing: New Horizons (fixed in v2.0.6)
- ARMS (fixed in v5.4.1)
- Splatoon (fixed in v2.12.1)
- Splatoon 2 (fixed in v5.5.1)
- Splatoon 3 (fixed in late 2022, exact version unknown)
- Super Mario Maker 2 (fixed in v3.0.2)
- Nintendo Switch Sports (fixed in late 2022, exact version unknown)

Muchos más juegos...

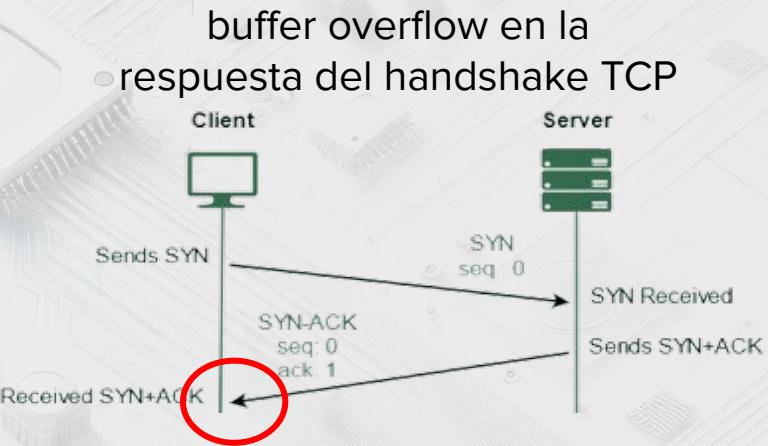
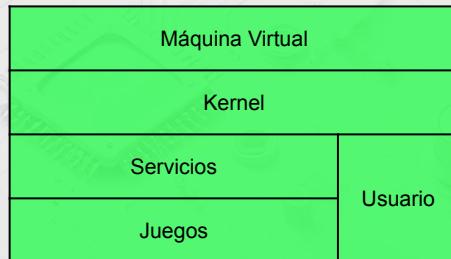
Broadpwn

Ahí no acaba la cosa

Módulo WiFi de la Nintendo Switch:

- Broadcom BCM4356
-  No ASLR
-  Toda la memoria RWX

Control total
desde aquí



```
if (tipo paquete == respuesta conexión)  
    memcpy(buffer, datos);
```

 No se comprueba el tamaño

Broadpwn

Broadcom BCM4356

- Con la vulnerabilidad
- También en:

Móviles



iPhone 5, 6, ...

IoT



Cámaras de seguridad

Coches



Tesla Model S



BMW Serie 7

Aviones



Boeing 787

RCM (Recovery Mode)

Vamos a hacer una demostración

Exploit RCM:

- Modo recuperación para cargar programas
- Se accede poniendo PIN 10 del JoyCon a Tierra (GND)

Fase muy temprana del arranque

- No ASLR todavía
- No se verifica el tamaño del programa



DEMO

Estamos
aquí



Ya ha habido casos...

Malware en:

- Nintendo Switch



FAKE POKEMON LET'S GO PIKACHU ROM BRICKS PIRATES' CONSOLES

November 16, 2018 Iggy 0 Comment

Last week, leaked copies of Pokemon Let's GO Eevee started circulating on the Internet after someone performed a ROM dump of the game.

Many pirates and users in the homebrew community used that as an opportunity to play.

PS3 Jailbreak Trojan (Aug 25, 2010)

By Security News

August 25, 2010

SonicWALL UTM Research team received reports of a new PS3 Jailbreak Trojan being distributed in the wild. This Trojan is actually a new variant of Trojan-Snare packaged together with a PS3 Jailbreak Tool. This tool

Wow, looks like someone made the first(?) 3DS malware ("UnbanMii"), steals console unique info from users:



gbatemp.net

ALL 3 Methods to get unbanned from recent ban wave

Nice to see that UnbanMii is used now :D == Update == ok, 2.0 *might* be released by today, the Team doesn't know ...

Tarde o temprano llegarán a consolas más modernas

Conclusión

-  **Ningún dispositivo** es **imposible de hackear** (Todavía no se ha descubierto cómo)
-  **Cualquier persona** puede hacerlo
-  Solo es **cuestión de tiempo** que alguien quiera **hacer el mal**
-  Una sola **vulnerabilidad** pueden afectar a **muchos dispositivos**
-  Podemos **prevenirnos**:
 - Evitar el pirateo
 - Conexiones a internet innecesarias



LinkedIn
Jose Fernández

¡ MUCHAS GRACIAS !