

27th Chaos Communication Congress

# Console Hacking 2010

PS3 Epic Fail

**fail0verflow**

bushing, marcan, segher, sven

# Who are we?

- In 2008 at 25c3 these teams worked together as 'WiiPhonies'
- We won the 25c3 CTF
- We changed our name to 'Fail Overflow'
  - Not trademark infringing
  - The domain was available
  - The ratio of fail to win is high.

We've been collaborating on various embedded and thought expansive projects, the most famous of which that hit the press earlier this year was the full reconstruction of the \$REDACTED allowing \$REDACTED to be completely broken, that was a fun couple of weeks.

# Wii had a good run

- 3 years, 9 firmware updates, 1 real feature
- 73 mil. consoles, 30 mil. vuln. bootloaders
- 1 million users of Homebrew Channel

# Wii      Xbox 360      PS3

2006

2007

2008

2009

2010

2011

t



# Wii      Xbox 360      PS3

2006

Drivechips

2007

Twiizer Attack

2008

Twilight Hack

Homebrew

Channel

2009

Bannerbomb

Indiana Pwns

Bannerbomb

for 4.2

2010

latest update

broken

2011

t



# Wii      Xbox 360      PS3

2006

Drivechips  
King Kong Hack

Drive firmware  
hacked

2007

Twiizer Attack

Twilight Hack  
Homebrew  
Channel

2009

Bannerbomb  
Indiana Pwns  
Bannerbomb  
for 4.2

JTAG Hack

2010

latest update  
broken

2011

t

# Wii      Xbox 360      PS3

2006

Drivechips  
King Kong Hack  
Drive firmware hacked

2007

Twiizer Attack

2008

Twilight Hack  
Homebrew Channel

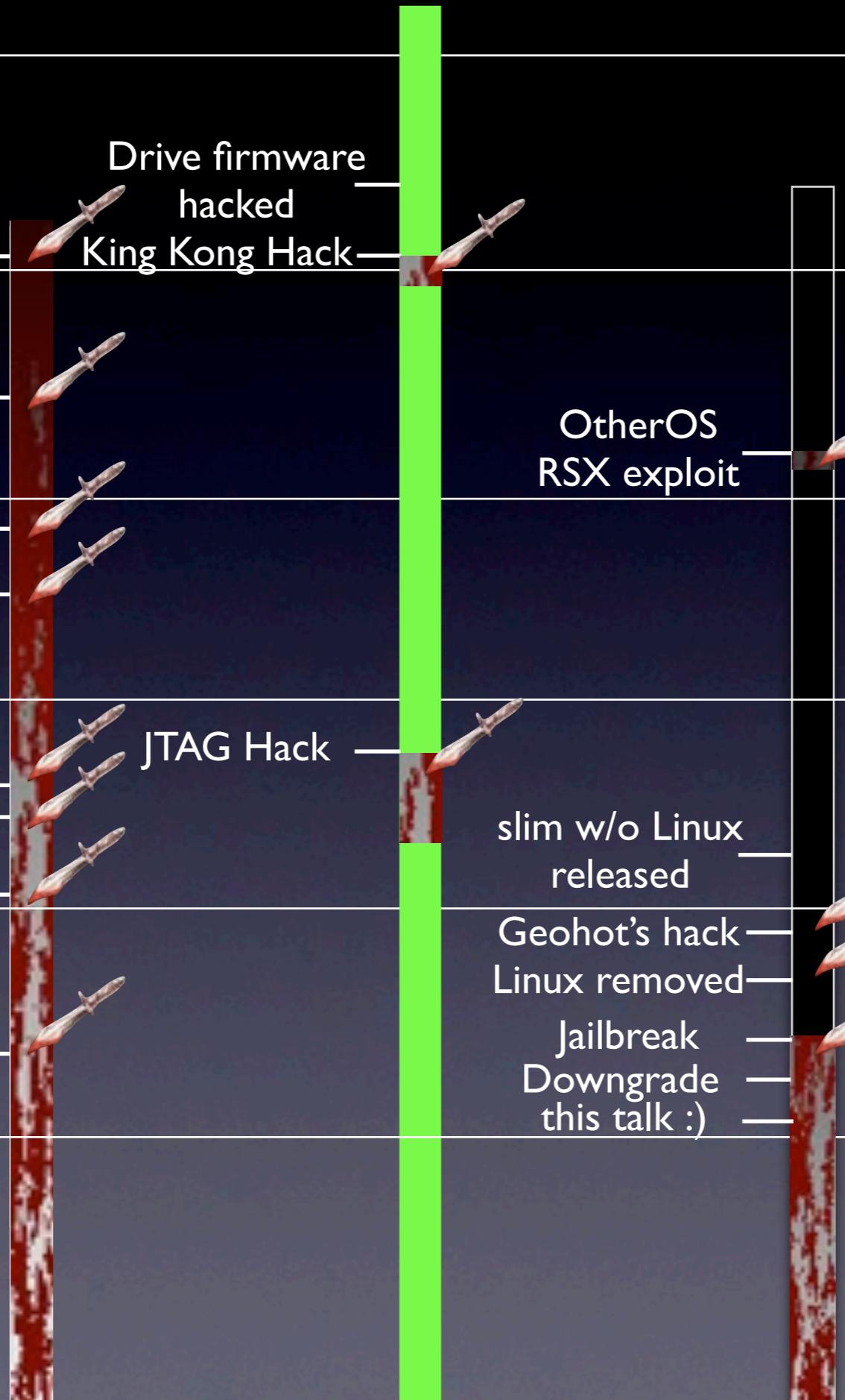
2009

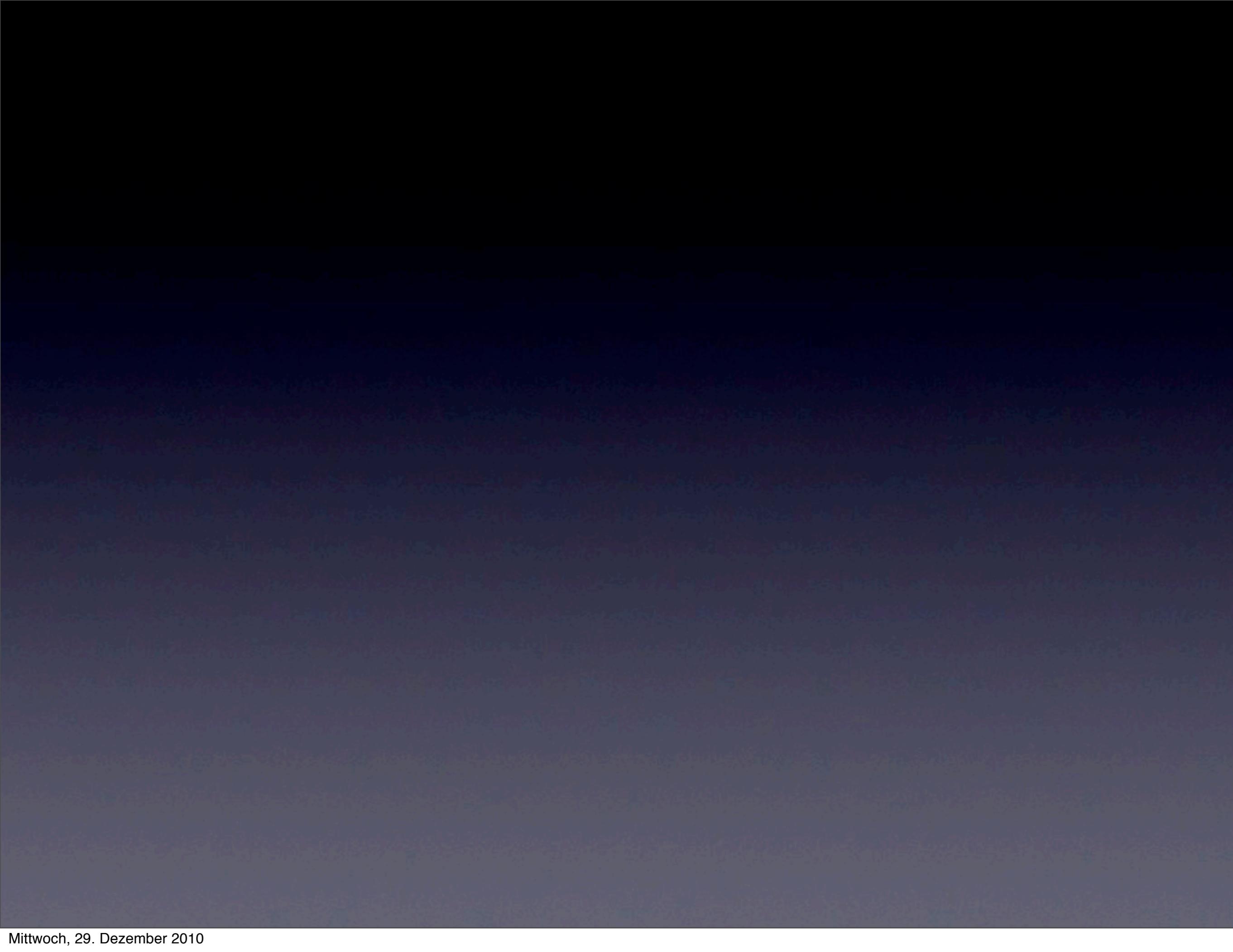
Bannerbomb  
Indiana Pwns  
Bannerbomb  
for 4.2

2010

latest update  
broken

2011





**device**

**PS2**

**dbox2**

**GameCube**

**Xbox**

**iPod**

**DS**

**PSP**

**Xbox 360**

**PS3**

**Wii**

**AppleTV**

**iPhone**

device	y
PS2	1999
dbox2	2000
GameCube	2001
Xbox	2001
iPod	2001
DS	2004
PSP	2004
Xbox 360	2005
PS3	2006
Wii	2006
AppleTV	2007
iPhone	2007

device	y	security
PS2	1999	?
dbox2	2000	signed kernel
GameCube	2001	encrypted boot
Xbox	2001	encrypted/signed bootup, signed executables
iPod	2001	checksum
DS	2004	signed/encrypted executables
PSP	2004	signed bootup/executables
Xbox 360	2005	encrypted/signed bootup, encrypted/signed executables, encrypted RAM, hypervisor, eFuses
PS3	2006	encrypted/signed bootup, encrypted/signed executables, hypervisor, eFuses, isolated SPU
Wii	2006	encrypted bootup
AppleTV	2007	signed bootloader
iPhone	2007	signed/encrypted bootup/executables

device	y	security	hacked
PS2	1999	?	?
dbox2	2000	signed kernel	3 months
GameCube	2001	encrypted boot	12 months
Xbox	2001	encrypted/signed bootup, signed executables	4 months
iPod	2001	checksum	<12 months
DS	2004	signed/encrypted executables	6 months
PSP	2004	signed bootup/executables	2 months
Xbox 360	2005	encrypted/signed bootup, encrypted/signed executables, encrypted RAM, hypervisor, eFuses	12 months
PS3	2006	encrypted/signed bootup, encrypted/signed executables, hypervisor, eFuses, isolated SPU	not yet
Wii	2006	encrypted bootup	1 month
AppleTV	2007	signed bootloader	2 weeks
iPhone	2007	signed/encrypted bootup/executables	11 days

device	y	security	hacked	for
<b>PS2</b>	1999	?	?	piracy
<b>dbox2</b>	2000	signed kernel	3 months	Linux
<b>GameCube</b>	2001	encrypted boot	12 months	Homebrew
<b>Xbox</b>	2001	encrypted/signed bootup, signed executables	4 months	Linux Homebrew
<b>iPod</b>	2001	checksum	<12 months	Linux
<b>DS</b>	2004	signed/encrypted executables	6 months	Homebrew
<b>PSP</b>	2004	signed bootup/executables	2 months	Homebrew
<b>Xbox 360</b>	2005	encrypted/signed bootup, encrypted/signed executables, encrypted RAM, hypervisor, eFuses	12 months	Linux Homebrew
<b>PS3</b>	2006	encrypted/signed bootup, encrypted/signed executables, hypervisor, eFuses, isolated SPU	not yet	-
<b>Wii</b>	2006	encrypted bootup	1 month	Linux
<b>AppleTV</b>	2007	signed bootloader	2 weeks	Linux
<b>iPhone</b>	2007	signed/encrypted bootup/executables	11 days	Homebrew, SIM-Lock

device	y	security	hacked	for	effect
<b>PS2</b>	1999	?	?	piracy	-
<b>dbox2</b>	2000	signed kernel	3 months	Linux	pay TV decoding
<b>GameCube</b>	2001	encrypted boot	12 months	Homebrew	piracy
<b>Xbox</b>	2001	encrypted/signed bootup, signed executables	4 months	Linux Homebrew	piracy
<b>iPod</b>	2001	checksum	<12 months	Linux	-
<b>DS</b>	2004	signed/encrypted executables	6 months	Homebrew	piracy
<b>PSP</b>	2004	signed bootup/executables	2 months	Homebrew	piracy
<b>Xbox 360</b>	2005	encrypted/signed bootup, encrypted/signed executables, encrypted RAM, hypervisor, eFuses	12 months	Linux Homebrew	leaked keys
<b>PS3</b>	2006	encrypted/signed bootup, encrypted/signed executables, hypervisor, eFuses, isolated SPU	not yet	-	-
<b>Wii</b>	2006	encrypted bootup	1 month	Linux	piracy
<b>AppleTV</b>	2007	signed bootloader	2 weeks	Linux	Front Row piracy
<b>iPhone</b>	2007	signed/encrypted bootup/executables	11 days	Homebrew, SIM-Lock	piracy

device	y	security	hacked	for	effect
<b>PS2</b>	1999	?	?	piracy	-
<b>dbox2</b>	2000	signed kernel	3 months	Linux	pay TV decoding
<b>GameCube</b>	2001	encrypted boot	12 months	Homebrew	piracy
<b>Xbox</b>	2001	encrypted/signed bootup, signed executables	4 months	Linux Homebrew	piracy
<b>iPod</b>	2001	checksum	<12 months	Linux	-
<b>DS</b>	2004	signed/encrypted executables	6 months	Homebrew	piracy
<b>PSP</b>	2004	signed bootup/executables	2 months	Homebrew	piracy
<b>Xbox 360</b>	2005	encrypted/signed bootup, encrypted/signed executables, encrypted RAM, hypervisor, eFuses	12 months	Linux Homebrew	leaked keys
<b>PS3</b>	2006	encrypted/signed bootup, encrypted/signed executables, hypervisor, eFuses, isolated SPU	not yet	-	-
<b>Wii</b>	2006	encrypted bootup	1 month	Linux	piracy
<b>AppleTV</b>	2007	signed bootloader	2 weeks	Linux	Front Row piracy
<b>iPhone</b>	2007	signed/encrypted bootup/executables	11 days	Homebrew, SIM-Lock	piracy
<b>iPad</b>	2010	signed/encrypted bootup/executables	1 day	Homebrew	piracy

device	y	security	hacked	for	effect
<b>PS2</b>	1999	?	?	piracy	-
<b>dbox2</b>	2000	signed kernel	3 months	Linux	pay TV decoding
<b>GameCube</b>	2001	encrypted boot	12 months	Homebrew	piracy
<b>Xbox</b>	2001	encrypted/signed bootup, signed executables	4 months	Linux Homebrew	piracy
<b>iPod</b>	2001	checksum	<12 months	Linux	-
<b>DS</b>	2004	signed/encrypted executables	6 months	Homebrew	piracy
<b>PSP</b>	2004	signed bootup/executables	2 months	Homebrew	piracy
<b>Xbox 360</b>	2005	encrypted/signed bootup, encrypted/signed executables, encrypted RAM, hypervisor, eFuses	12 months	Linux Homebrew	leaked keys
<b>PS3</b>	2006	encrypted/signed bootup, encrypted/signed executables, hypervisor, eFuses, isolated SPU	not yet	-	-
<b>Wii</b>	2006	encrypted bootup	1 month	Linux	piracy
<b>AppleTV</b>	2007	signed bootloader	2 weeks	Linux	Front Row piracy
<b>iPhone</b>	2007	signed/encrypted bootup/executables	11 days	Homebrew, SIM-Lock	piracy
<b>iPad</b>	2010	signed/encrypted bootup/executables	1 day	Homebrew	piracy

device	y	security	hacked	for	effect
PS2	1999	?	?	piracy	-
dbox2	2000	signed kernel	3 months	Linux	pay TV decoding
GameCube	2001	encrypted boot	12 months	Homebrew	piracy
Xbox	2001	encrypted/signed bootup, signed executables	4 months	Linux Homebrew	piracy
iPod	2001	checksum	<12 months	Linux	-
DS	2004	signed/encrypted executables	6 months	Homebrew	piracy
PSP	2004	signed bootup/executables	2 months	Homebrew	piracy
Xbox 360	2005	encrypted/signed bootup, encrypted/signed executables, encrypted RAM, hypervisor, eFuses	12 months	Linux Homebrew	leaked keys
PS3	2006	encrypted/signed bootup, encrypted/signed executables, hypervisor, eFuses, isolated SPU	4 years	-	-
Wii	2006	encrypted bootup	1 month	Linux	piracy
AppleTV	2007	signed bootloader	2 weeks	Linux	Front Row piracy
iPhone	2007	signed/encrypted bootup/executables	11 days	Homebrew, SIM-Lock	piracy
iPad	2010	signed/encrypted bootup/executables	1 day	Homebrew	piracy

device	y	security	hacked	for	effect
PS2	1999	?	?	piracy	-
dbox2	2000	signed kernel	3 months	Linux	pay TV decoding
GameCube	2001	encrypted boot	12 months	Homebrew	piracy
Xbox	2001	encrypted/signed bootup, signed executables	4 months	Linux Homebrew	piracy
iPod	2001	checksum	<12 months	Linux	-
DS	2004	signed/encrypted executables	6 months	Homebrew	piracy
PSP	2004	signed bootup/executables	2 months	Homebrew	piracy
Xbox 360	2005	encrypted/signed bootup, encrypted/signed executables, encrypted RAM, hypervisor, eFuses	12 months	Linux Homebrew	leaked keys
PS3	2006	encrypted/signed bootup, encrypted/signed executables, hypervisor, eFuses, isolated SPU	4 years	Homebrew Piracy	-
Wii	2006	encrypted bootup	1 month	Linux	piracy
AppleTV	2007	signed bootloader	2 weeks	Linux	Front Row piracy
iPhone	2007	signed/encrypted bootup/executables	11 days	Homebrew, SIM-Lock	piracy
iPad	2010	signed/encrypted bootup/executables	1 day	Homebrew	piracy

device	y	security	hacked	for	effect
<b>PS2</b>	1999	?	?	piracy	-
<b>dbox2</b>	2000	signed kernel	3 months	Linux	pay TV decoding
<b>GameCube</b>	2001	encrypted boot	12 months	Homebrew	piracy
<b>Xbox</b>	2001	encrypted/signed bootup, signed executables	4 months	Linux Homebrew	piracy
<b>iPod</b>	2001	checksum	<12 months	Linux	-
<b>DS</b>	2004	signed/encrypted executables	6 months	Homebrew	piracy
<b>PSP</b>	2004	signed bootup/executables	2 months	Homebrew	piracy
<b>Xbox 360</b>	2005	encrypted/signed bootup, encrypted/signed executables, encrypted RAM, hypervisor, eFuses	12 months	Linux Homebrew	leaked keys
<b>PS3</b>	2006	encrypted/signed bootup, encrypted/signed executables, hypervisor, eFuses, isolated SPU	4 years	Homebrew Piracy	piracy
<b>Wii</b>	2006	encrypted bootup	1 month	Linux	piracy
<b>AppleTV</b>	2007	signed bootloader	2 weeks	Linux	Front Row piracy
<b>iPhone</b>	2007	signed/encrypted bootup/executables	11 days	Homebrew, SIM-Lock	piracy
<b>iPad</b>	2010	signed/encrypted bootup/executables	1 day	Homebrew	piracy

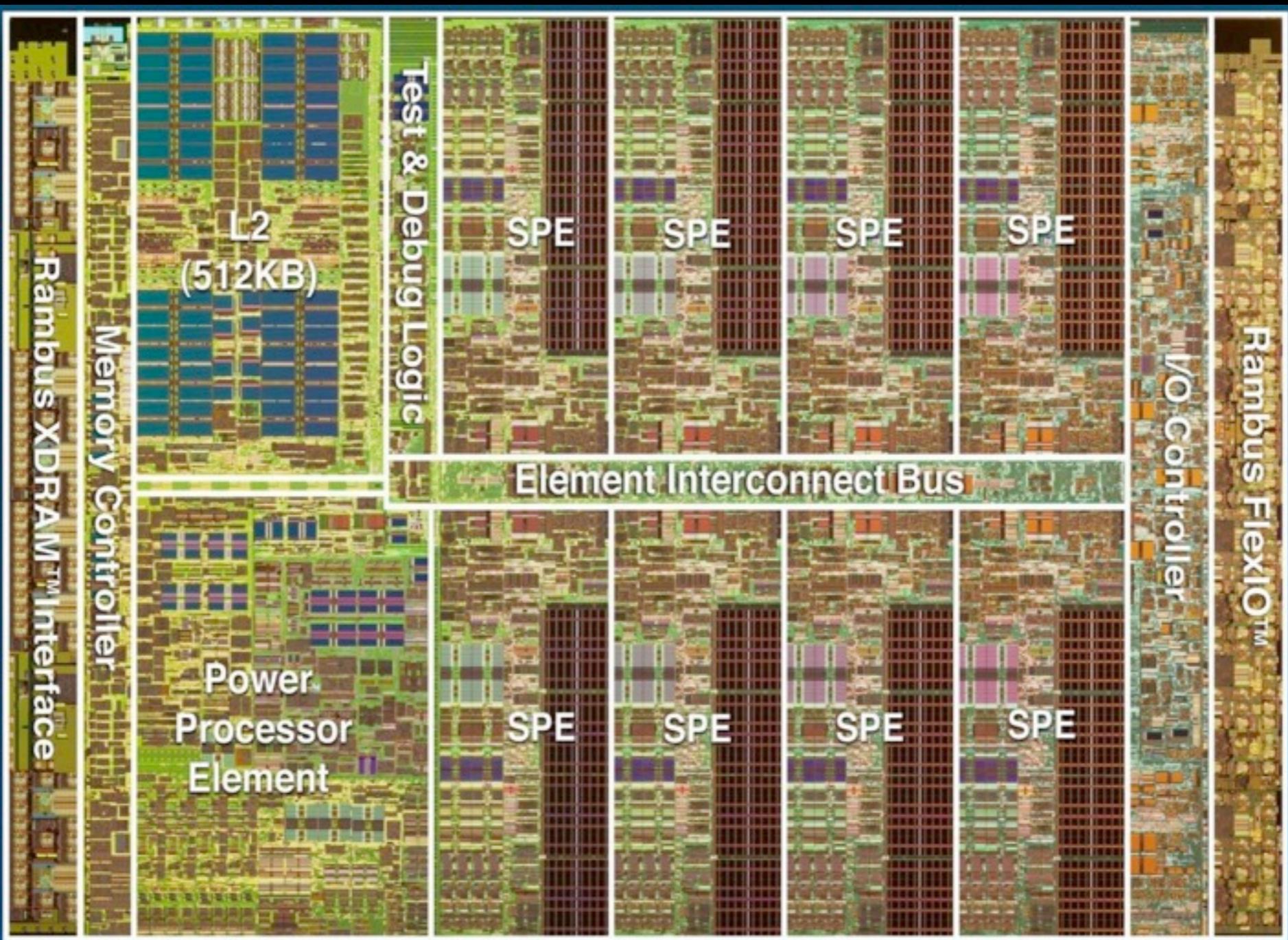
device	y	security	hacked	for	effect
<b>PS2</b>	1999	?	?	piracy	-
<b>dbox2</b>	2000	signed kernel	3 months	Linux	pay TV decoding
<b>GameCube</b>	2001	encrypted boot	12 months	Homebrew	piracy
<b>Xbox</b>	2001	encrypted/signed bootup, signed executables	4 months	Linux Homebrew	piracy
<b>iPod</b>	2001	checksum	<12 months	Linux	-
<b>DS</b>	2004	signed/encrypted executables	6 months	Homebrew	piracy
<b>PSP</b>	2004	signed bootup/executables	2 months	Homebrew	piracy
<b>Xbox 360</b>	2005	encrypted/signed bootup, encrypted/signed executables, encrypted RAM, hypervisor, eFuses	12 months	Linux Homebrew	leaked keys
<b>PS3</b>	2006	encrypted/signed bootup, encrypted/signed executables, hypervisor, eFuses, isolated SPU	4 years	Homebrew Piracy	piracy
<b>Wii</b>	2006	encrypted bootup	1 month	Linux	piracy
<b>AppleTV</b>	2007	signed bootloader	2 weeks	Linux	Front Row piracy
<b>iPhone</b>	2007	signed/encrypted bootup/executables	11 days	Homebrew, SIM-Lock	piracy
<b>iPad</b>	2010	signed/encrypted bootup/executables	1 day	Homebrew	piracy

device	y	security	hacked after it was closed	or	effect
PS2	1999	?	?	piracy	-
dbox2	2000	signed kernel	3 months	Linux	pay TV decoding
GameCube	2001	encrypted boot	12 months	Homebrew	piracy
Xbox	2001	encrypted/signed bootup, signed executables	4 months	Linux Homebrew	piracy
iPod	2001	checksum	<12 months	Linux	-
DS	2004	signed/encrypted executables	6 months	Homebrew	piracy
PSP	2004	signed bootup/executables	2 months	Homebrew	piracy
Xbox 360	2005	encrypted/signed bootup, encrypted/signed executables, encrypted RAM, hypervisor, eFuses	12 months	Linux Homebrew	leaked keys
PS3	2006	encrypted/signed bootup, encrypted/signed executables, hypervisor, eFuses, isolated SPU	4 years	Homebrew Piracy	piracy
Wii	2006	encrypted bootup	1 month	Linux	piracy
AppleTV	2007	signed bootloader	2 weeks	Linux	Front Row piracy
iPhone	2007	signed/encrypted bootup/executables	11 days	Homebrew, SIM-Lock	piracy
iPad	2010	signed/encrypted bootup/executables	1 day	Homebrew	piracy

device	y	security	hacked after it was closed	or	effect
PS2	1999	?	?	piracy	-
dbox2	2000	signed kernel	3 months	Linux	pay TV decoding
GameCube	2001	encrypted boot	12 months	Homebrew	piracy
Xbox	2001	encrypted/signed bootup, signed executables	4 months	Linux Homebrew	piracy
iPod	2001	checksum	<12 months	Linux	-
DS	2004	signed/encrypted executables	6 months	Homebrew	piracy
PSP	2004	signed bootup/executables	2 months	Homebrew	piracy
Xbox 360	2005	encrypted/signed bootup, encrypted/signed executables, encrypted RAM, hypervisor, eFuses	12 months	Linux Homebrew	leaked keys
PS3	2006	encrypted/signed bootup, encrypted/signed executables, hypervisor, eFuses, isolated SPU	12 months	Homebrew Piracy	piracy
Wii	2006	encrypted bootup	1 month	Linux	piracy
AppleTV	2007	signed bootloader	2 weeks	Linux	Front Row piracy
iPhone	2007	signed/encrypted bootup/executables	11 days	Homebrew, SIM-Lock	piracy
iPad	2010	signed/encrypted bootup/executables	1 day	Homebrew	piracy

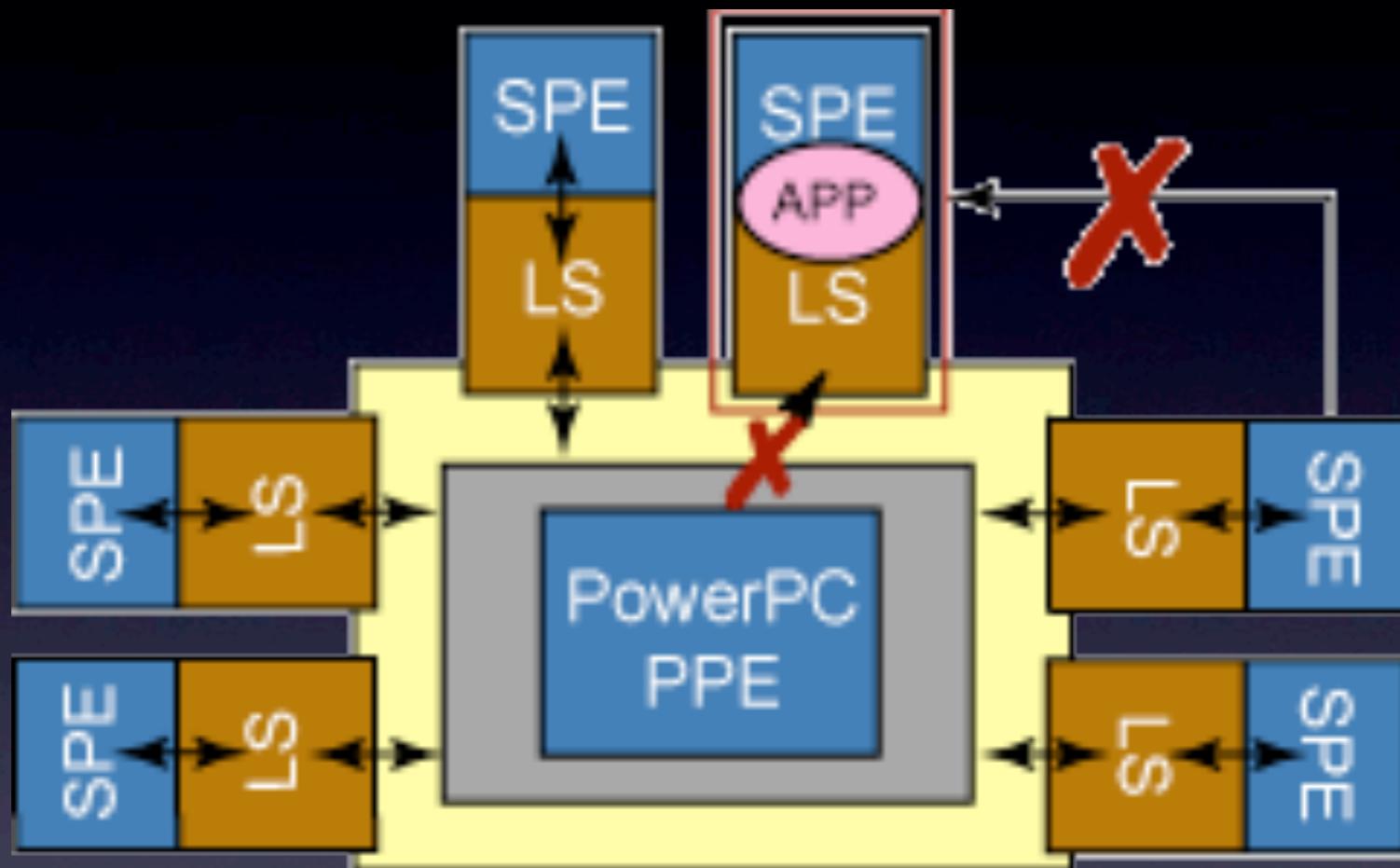
# PS3 Architecture

# The Cell Broadband Engine

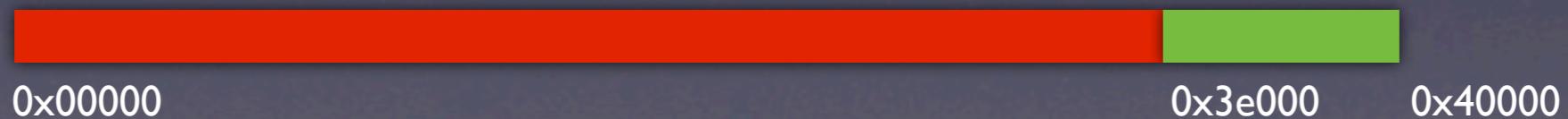


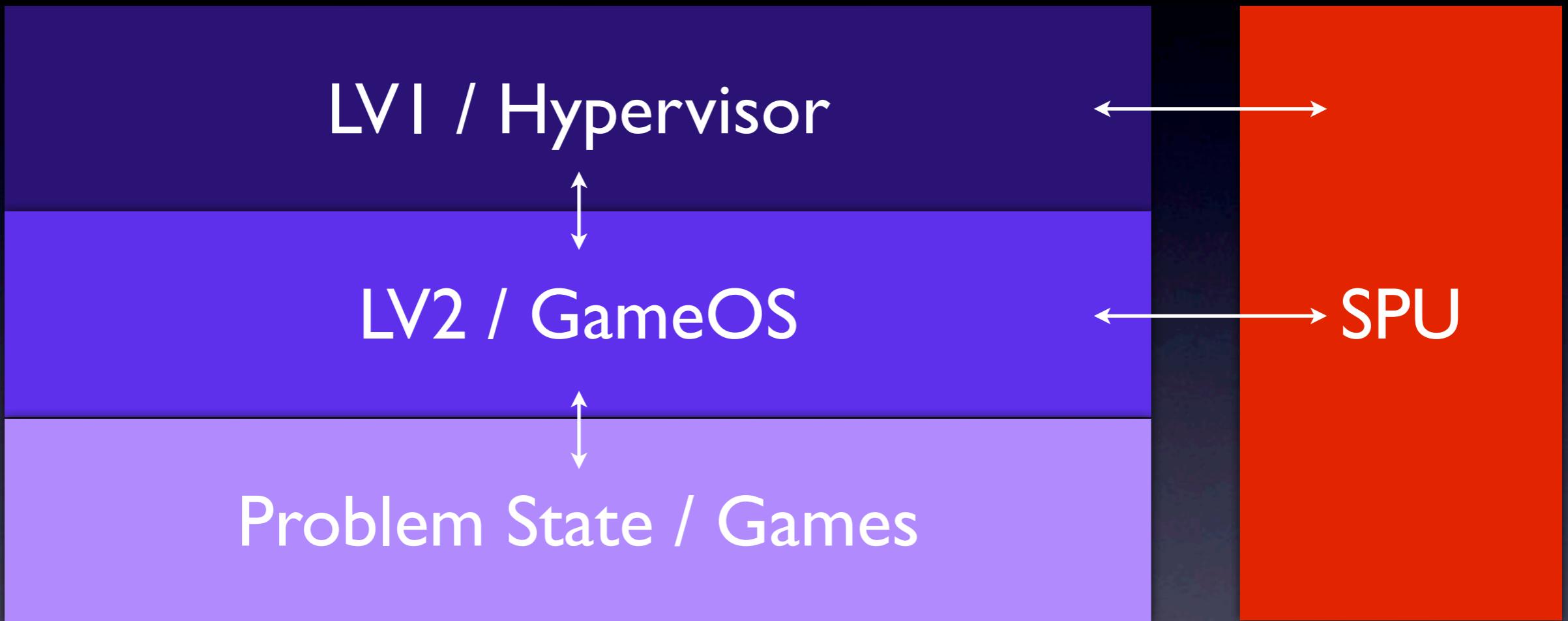
Source: IBM

# SPU Isolation



Source: IBM



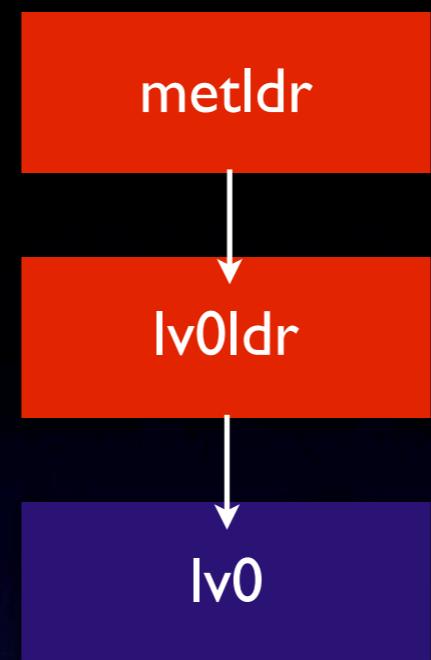


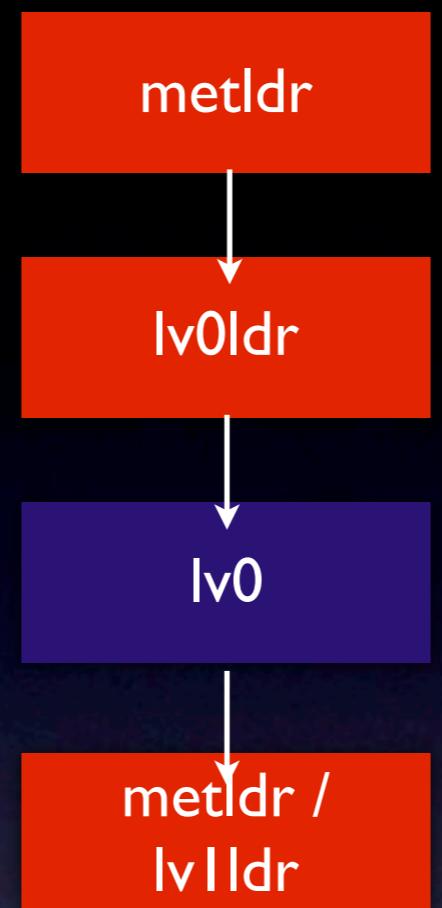
metldr

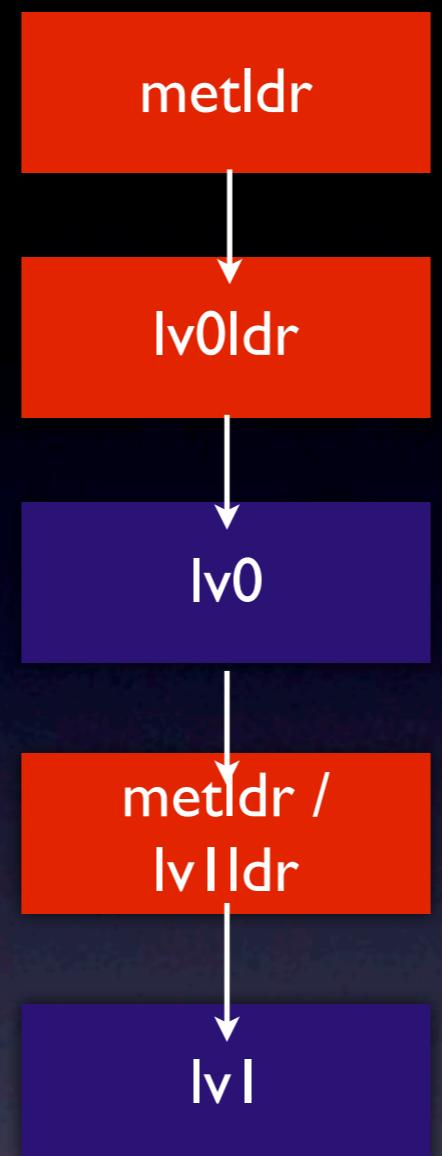
metldr

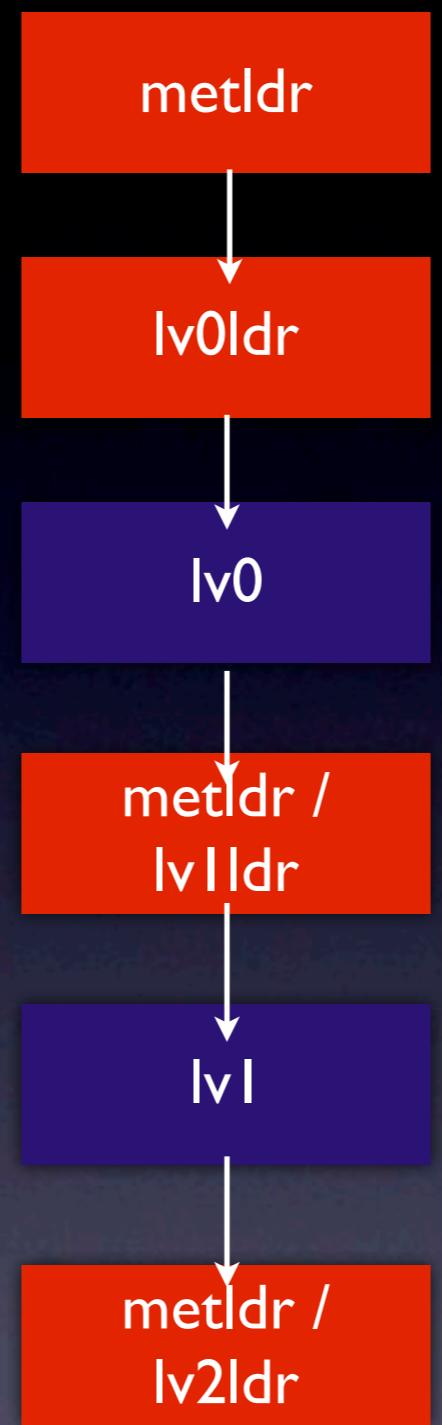


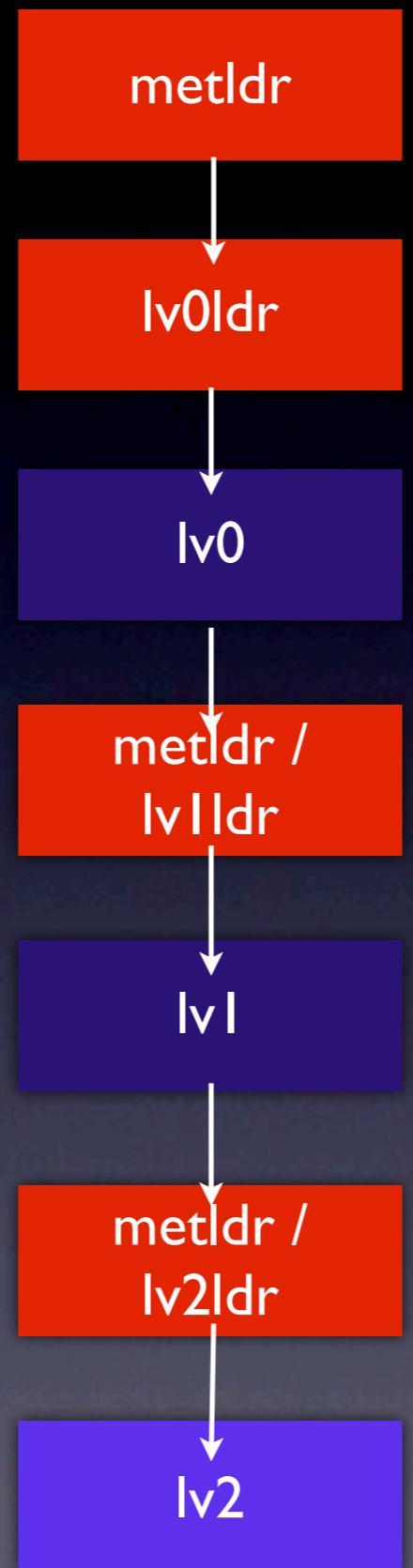
lv0ldr

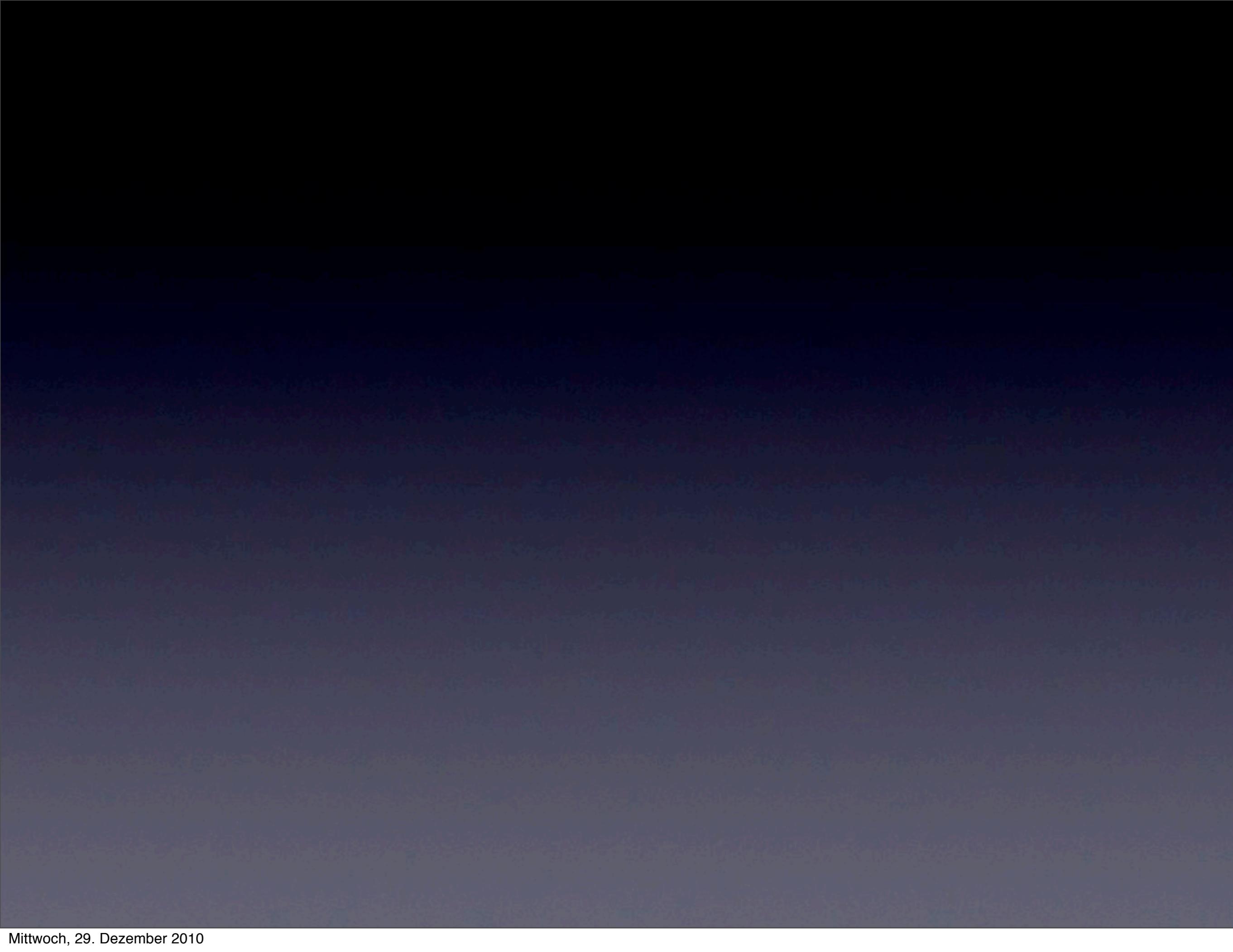












Xbox

Wii

360

PS3

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓
Security coprocessor		✓		✓

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓
Security coprocessor		✓		✓
Full media encryption and signing	✓			
Encrypted storage		✓		✓

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		
Encrypted storage		✓		✓
Self-signed storage		✓		

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		
Encrypted storage		✓		✓
Self-signed storage		✓		
Memory encryption/hashing			✓	

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		
Encrypted storage		✓		✓
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	✓

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		
Encrypted storage		✓		✓
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	✓
User/kernelmode				✓

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		
Encrypted storage		✓		✓
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	✓
User/kernelmode				✓
Anti-downgrade eFUSES			✓	

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		
Encrypted storage		✓		BYPASSED
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	✓
User/kernelmode				✓
Anti-downgrade eFUSES			✓	

# OtherOS



Not supported on the PS3 Slim



You have earned a trophy.  
🏆 Draw Attention

Otkros

Not supported on the PS3 Slim

# Geohot Exploit

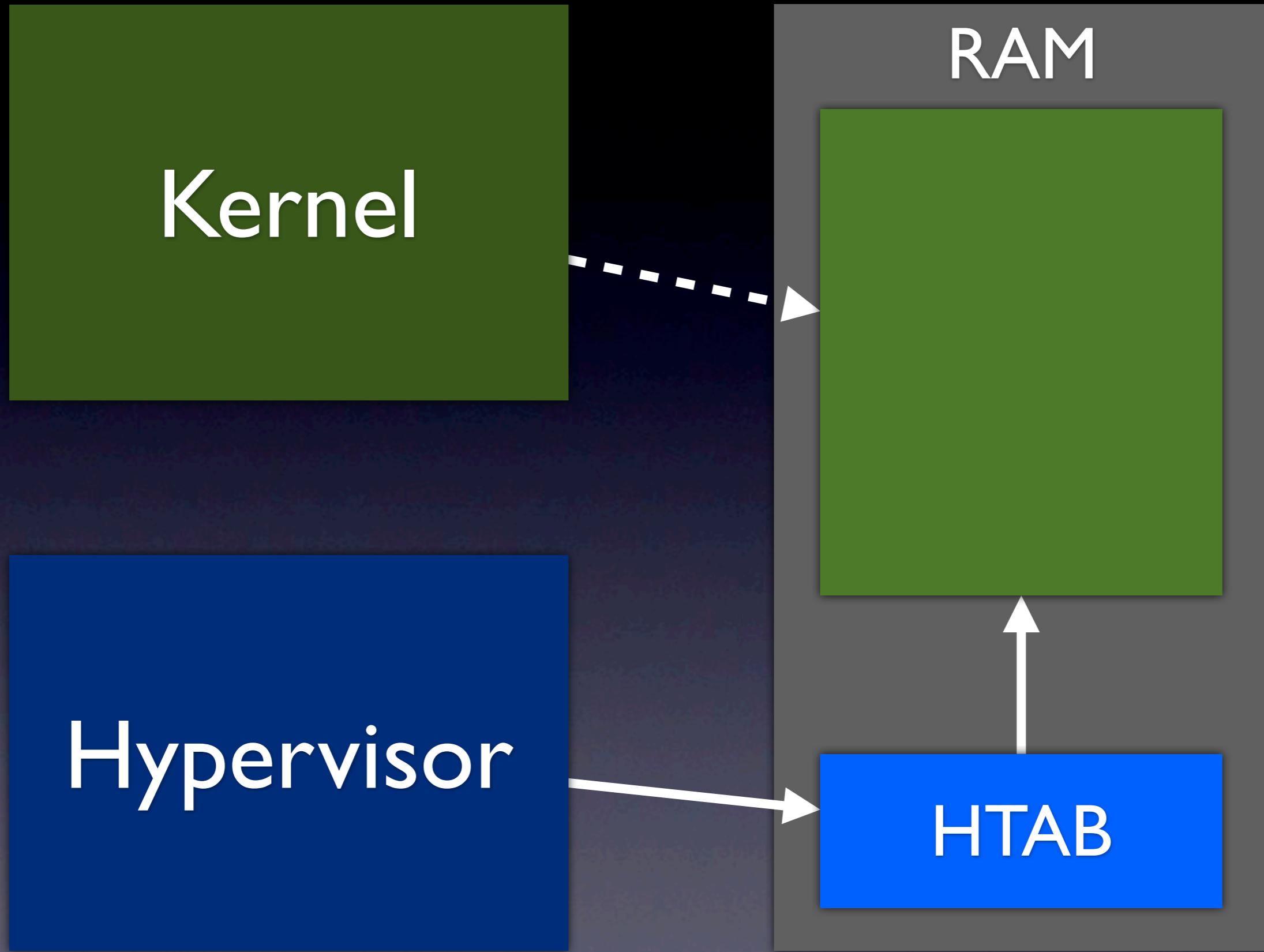
## XDR RAM Glitching Attack

Kernel

Hypervisor

RAM

HTAB

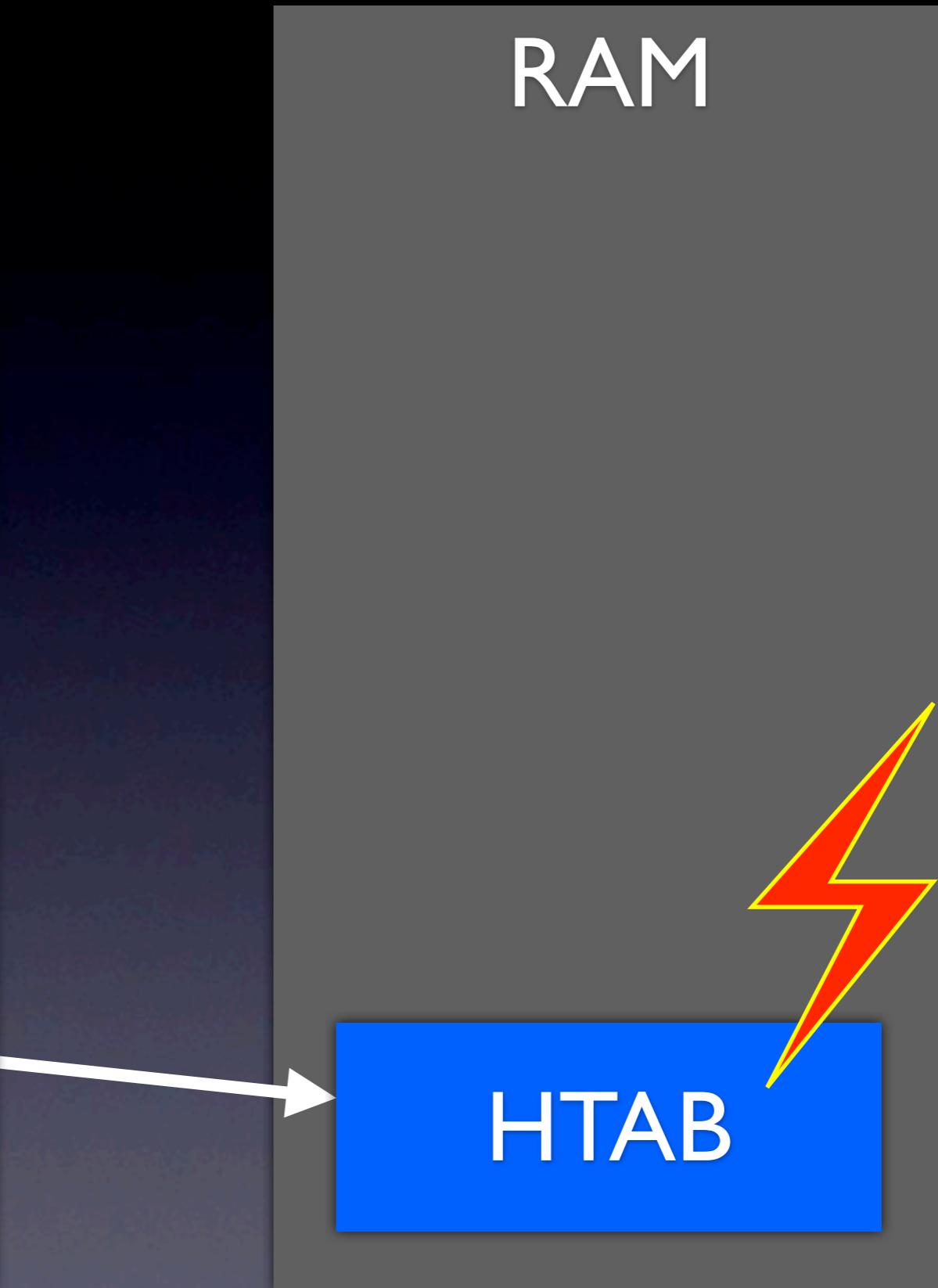


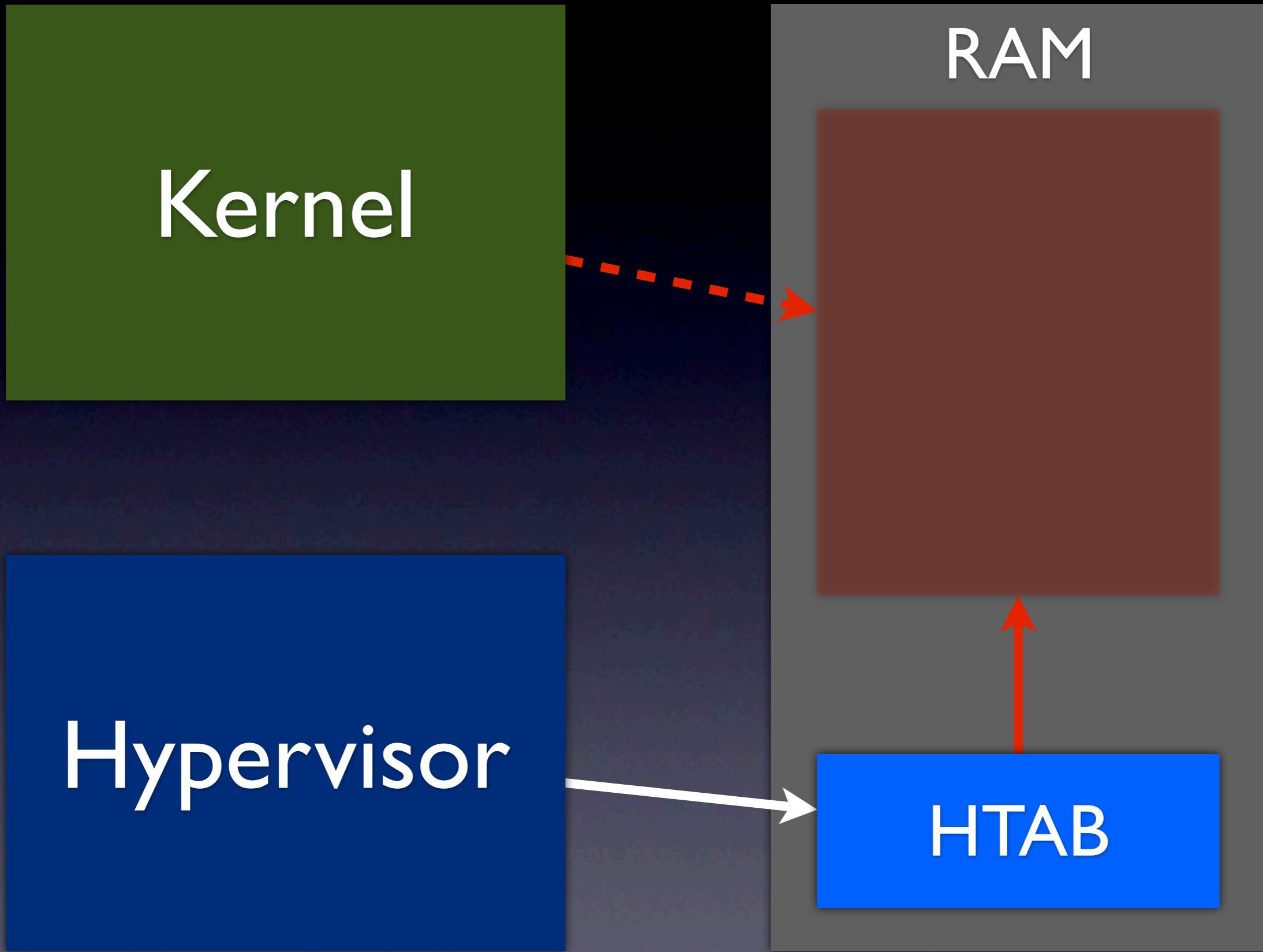
Kernel

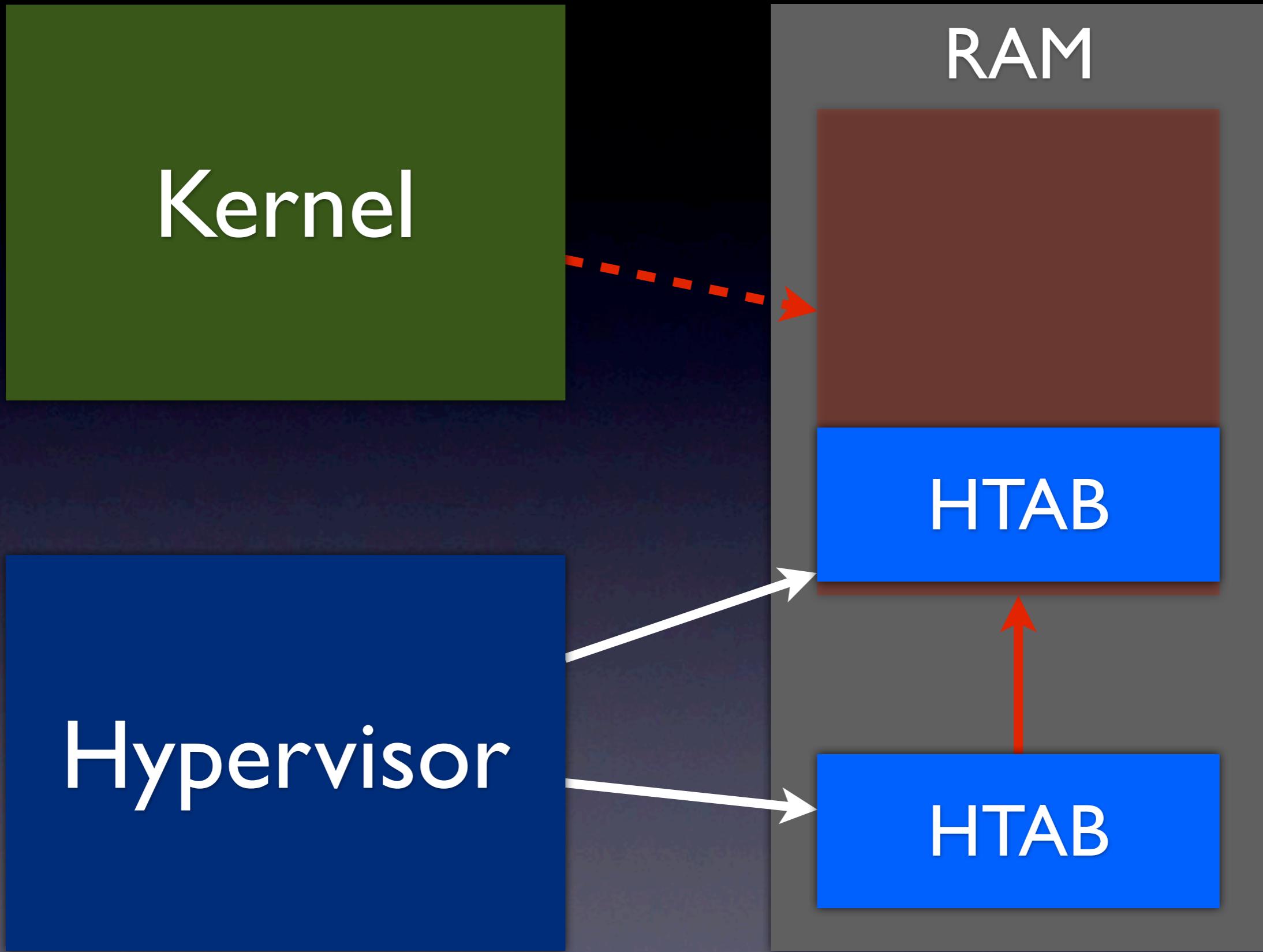
Hypervisor

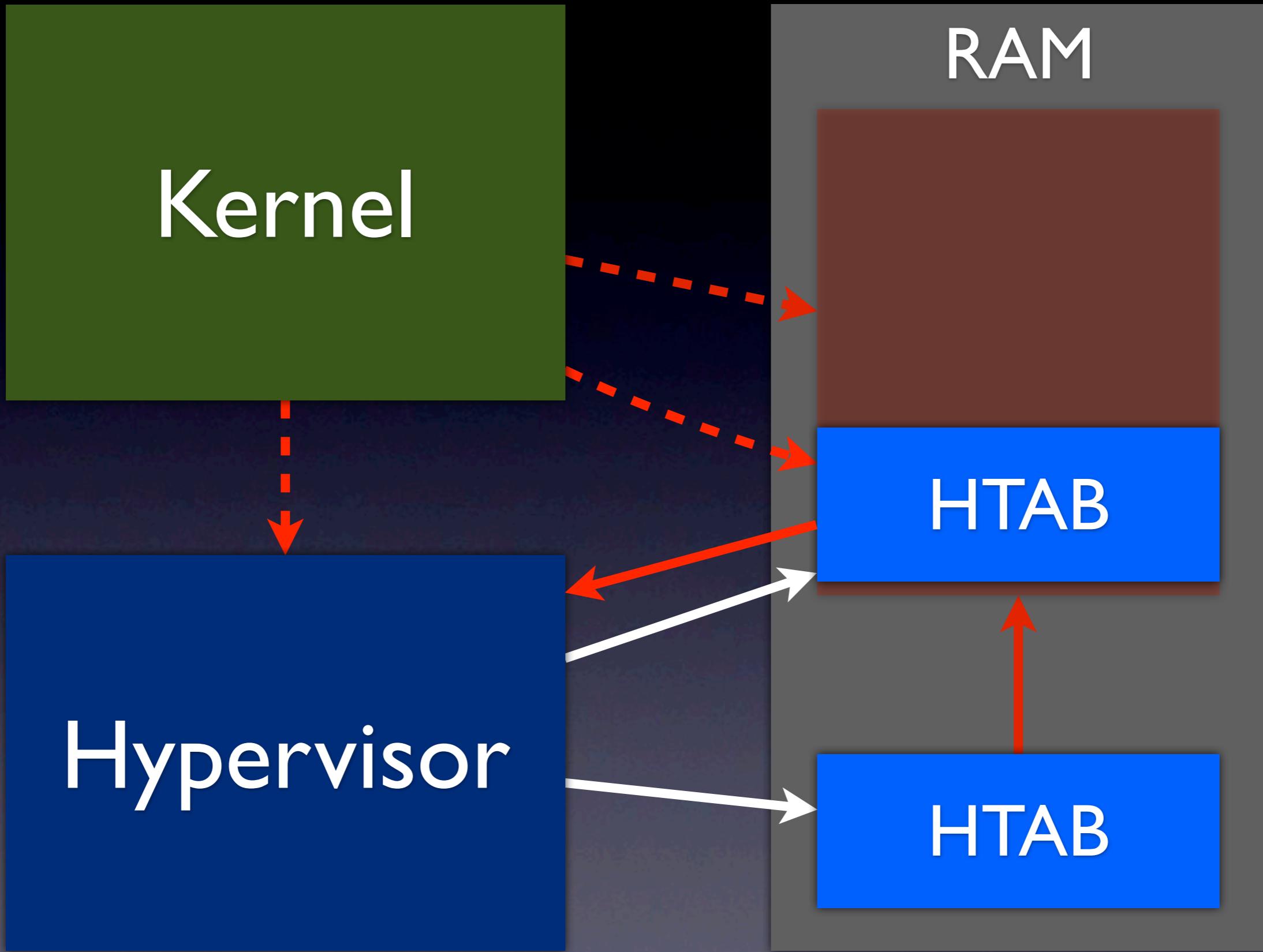
RAM

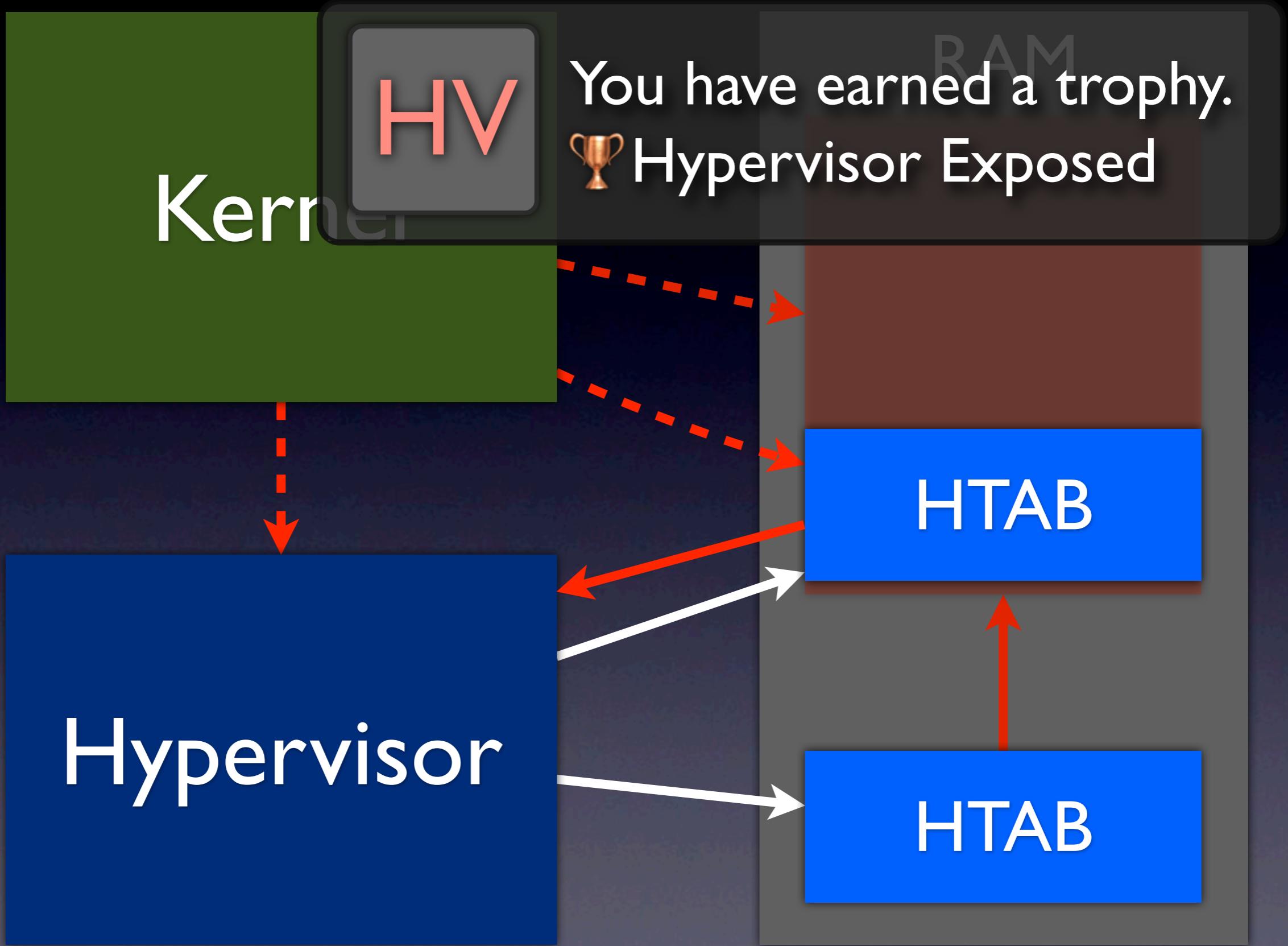
HTAB









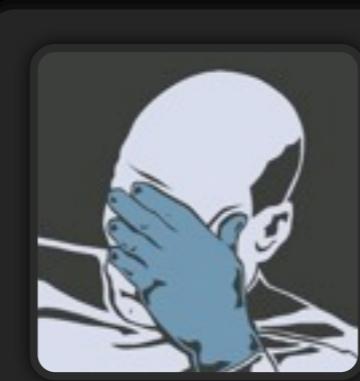


OtkROS





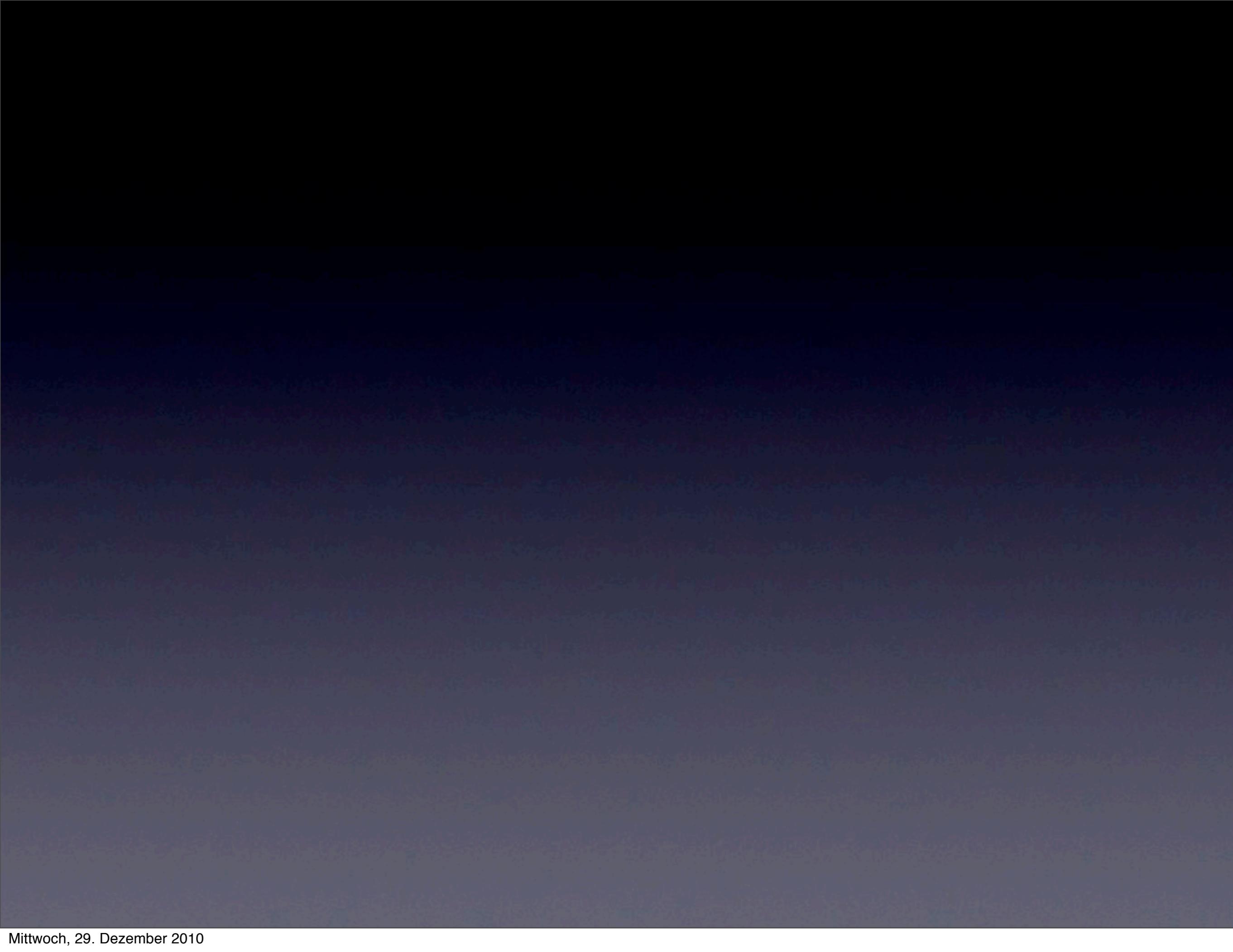
Forcibly removed on the PS3 Fat



You have earned a trophy.  
🏆 Pissed Off Hackers



Forcibly removed on the PS3 Fat



# PSJailbreak



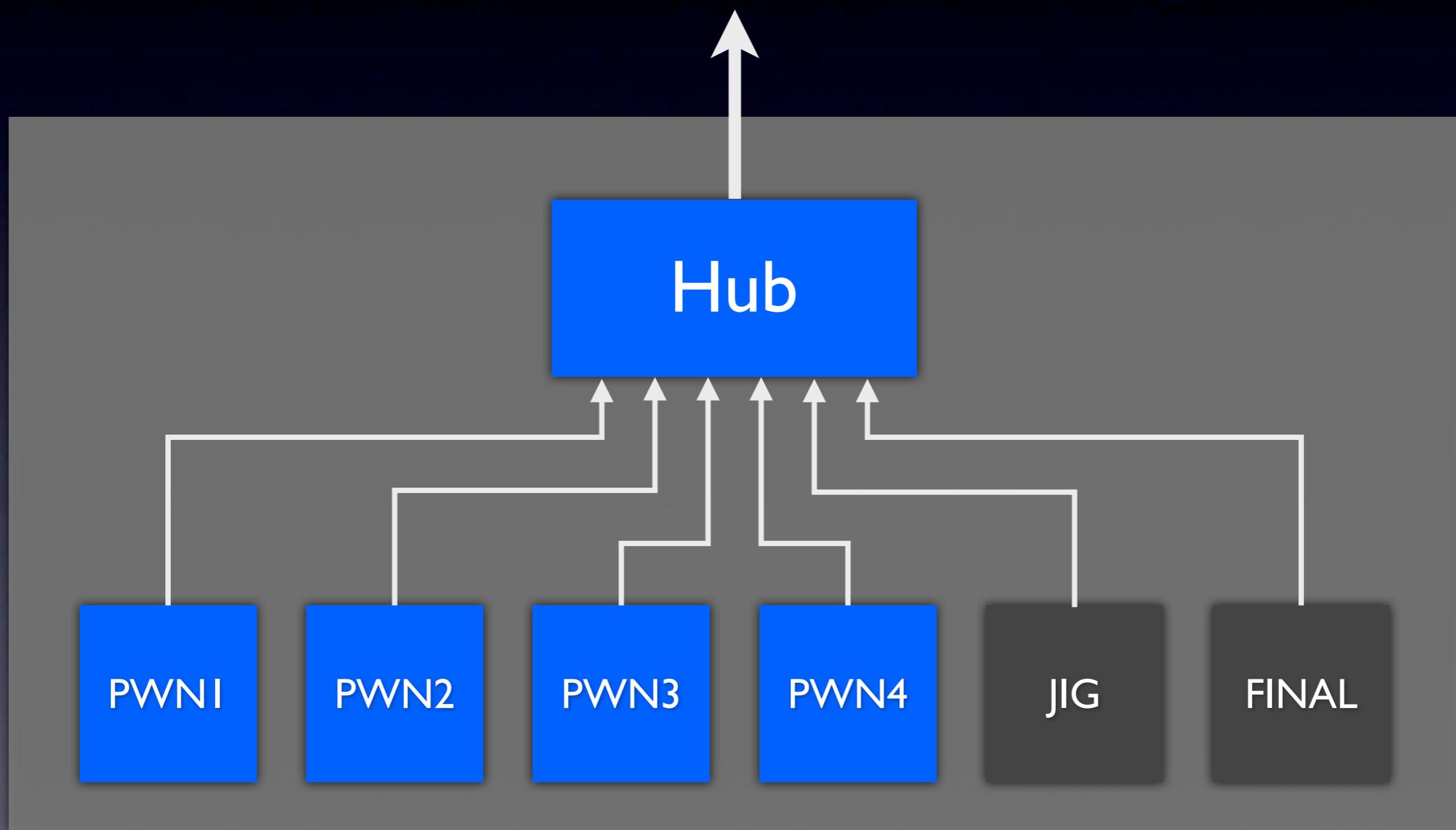
# PSJailbreak



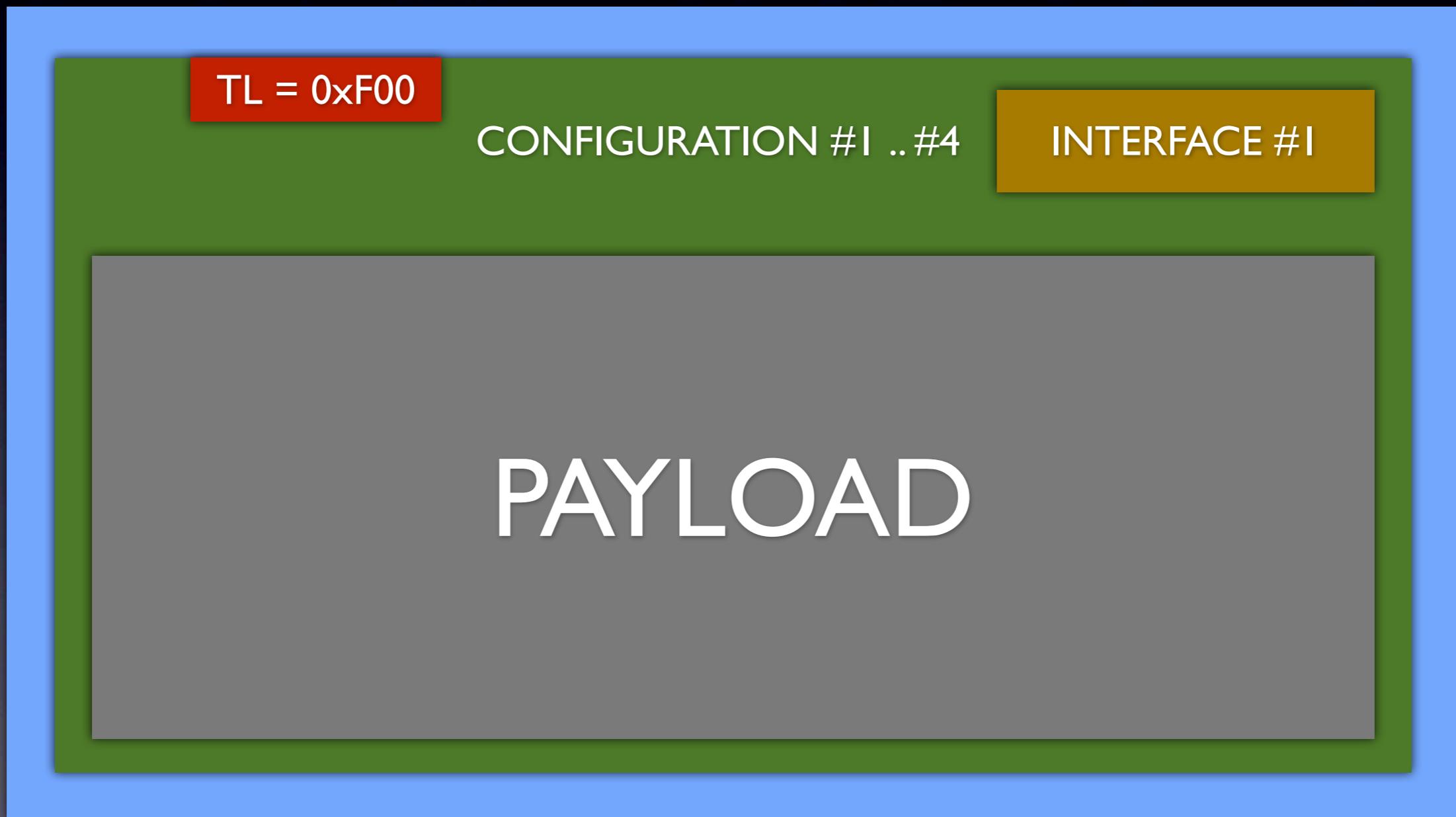
(And over 9000 clones)

# PSJailbreak Exploit

# PSJailbreak



# Device I



# Device 4



# Device 4

TL = 0x12

CONFIGURATION #1

INTERFACE #1

# Device 4

TL = 0x12

CONFIGURATION #1

INTERFACE #1

CONFIGURATION #2

# Device 2

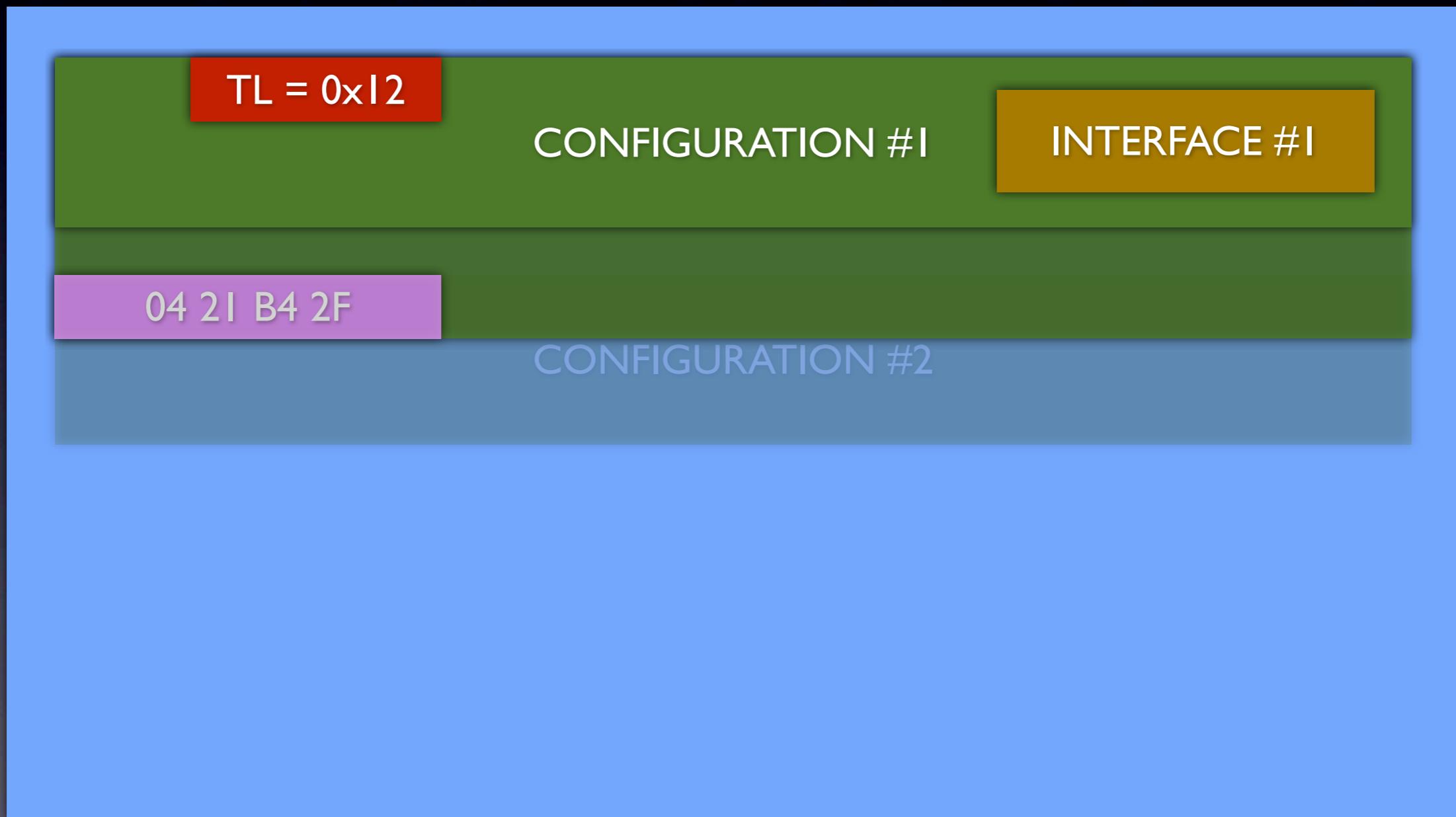
TL = 0x16

INTERFACE #1

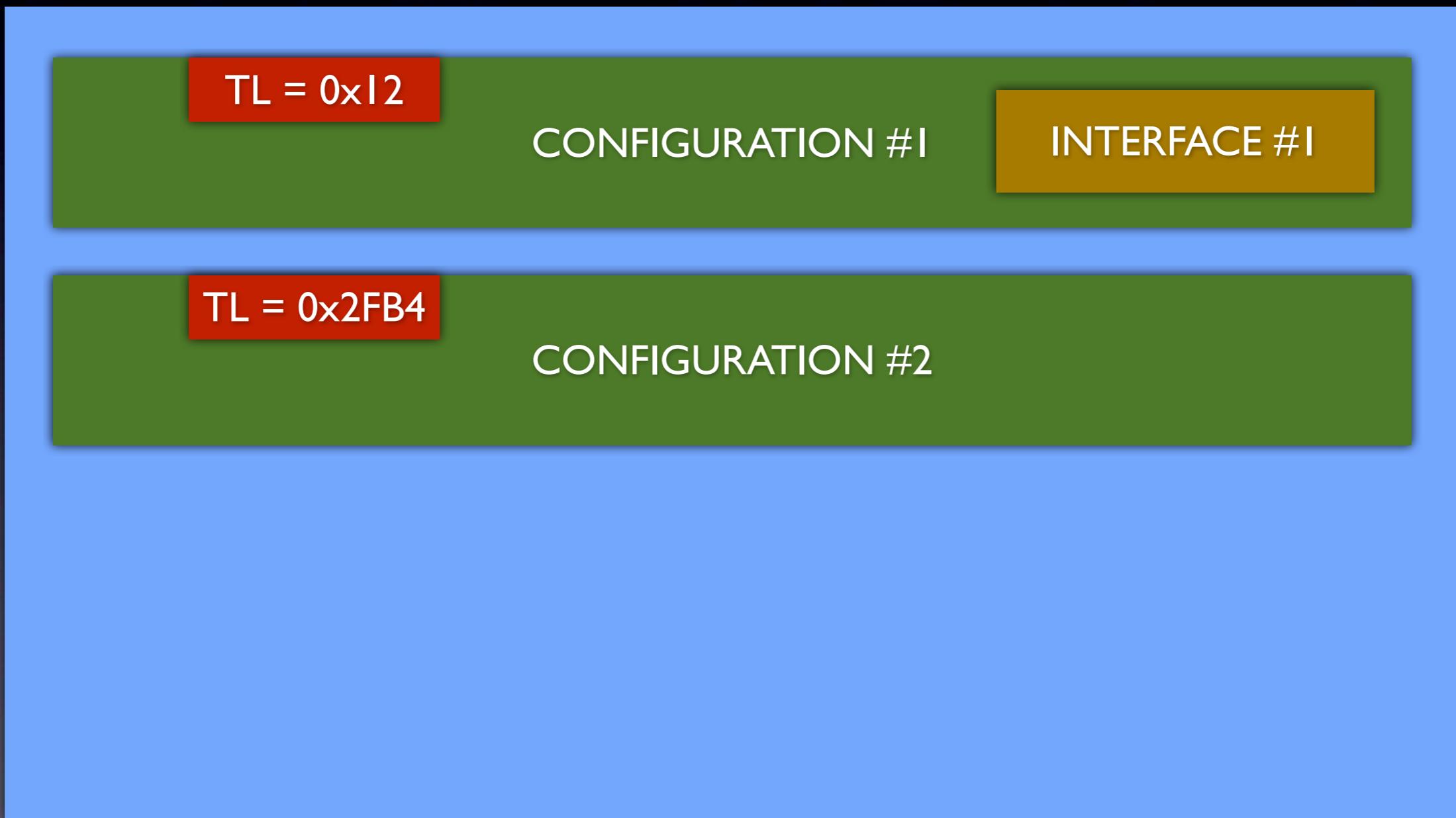
CONFIGURATION #1

04 21 B4 2F

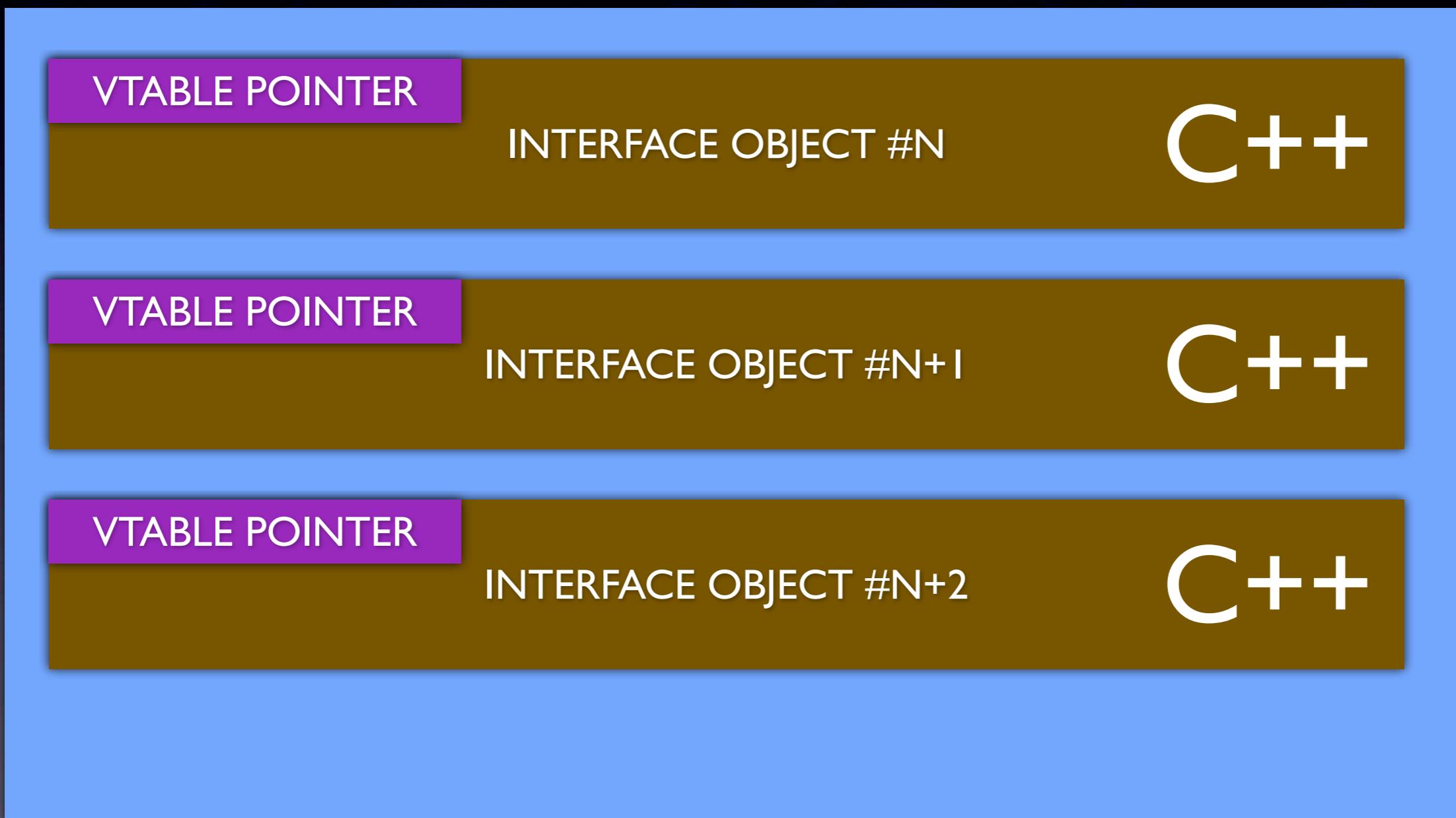
# Device 4



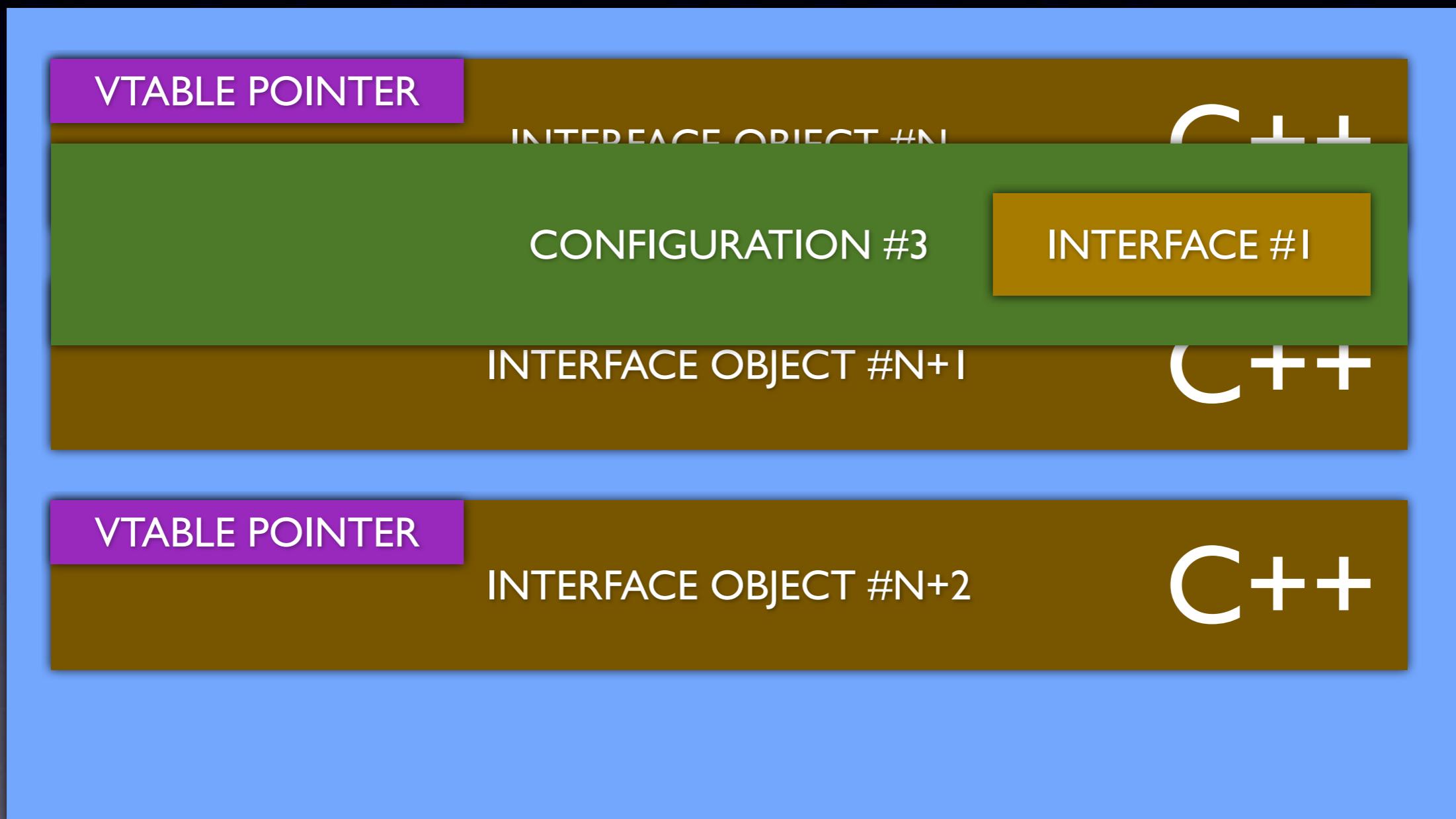
# Device 4



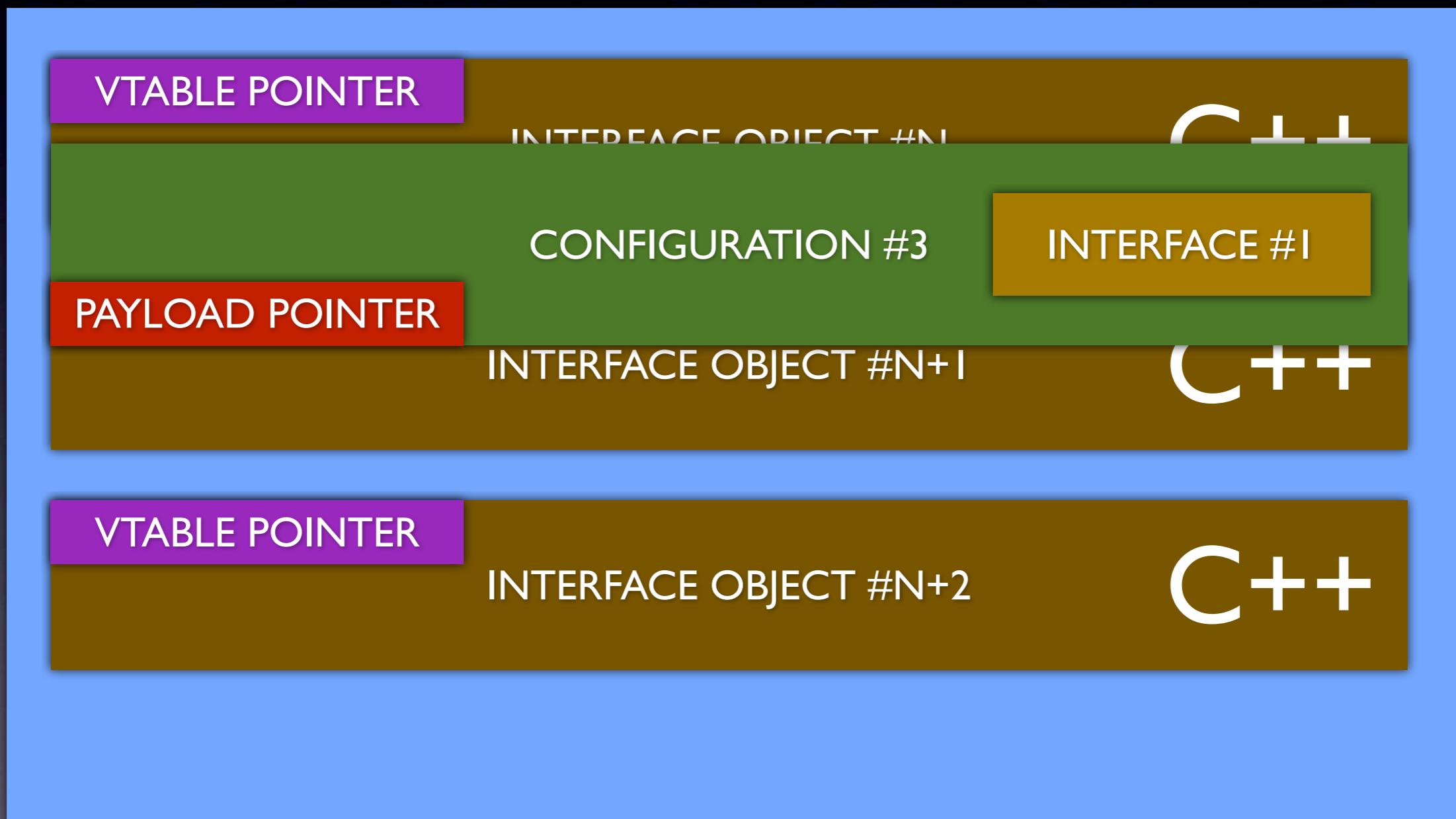
# C++ Objects



# C++ Objects



# C++ Objects



# Device 3

CONFIGURATION #1 .. #2

INTERFACE #1

INTERFACE #2

INTERFACE #3

INTERFACE #4

INTERFACE #5

INTERFACE #6

INTERFACE #7

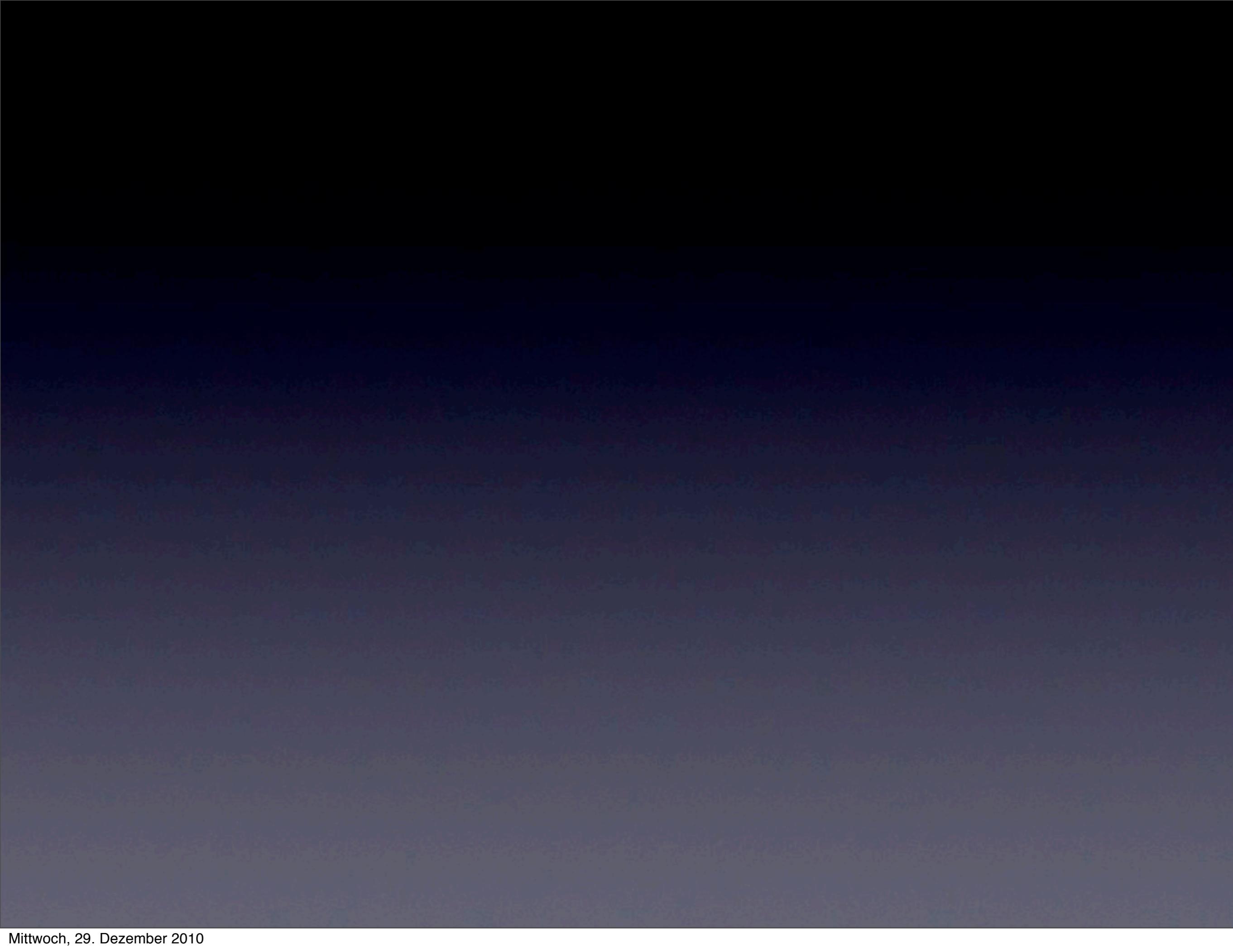
INTERFACE #8

INTERFACE #9

INTERFACE #10

INTERFACE #11

.....



```
addi sp, sp, 0  
ld r0, 0x10(s  
mtlr r0  
li r3, 0  
blr
```

You have earned a trophy.  
 LV2 Code Execution

# NO W<sup>A</sup>X in LV2

Any old exploit == code execution

# Hypervisor allows unsigned code

It happily marks pages as executable and plays no role  
in enforcing that only trusted code runs

# Results

- LV2 “GameOS” compromised
- LVI Hypervisor NOT compromised
- Secure SPE NOT compromised



You have earned a trophy.  
Piracy

- LV2 “GameOS” compromised
- LVI Hypervisor NOT compromised
- Secure SPE NOT compromised
- Piracy

# Fail Security Model

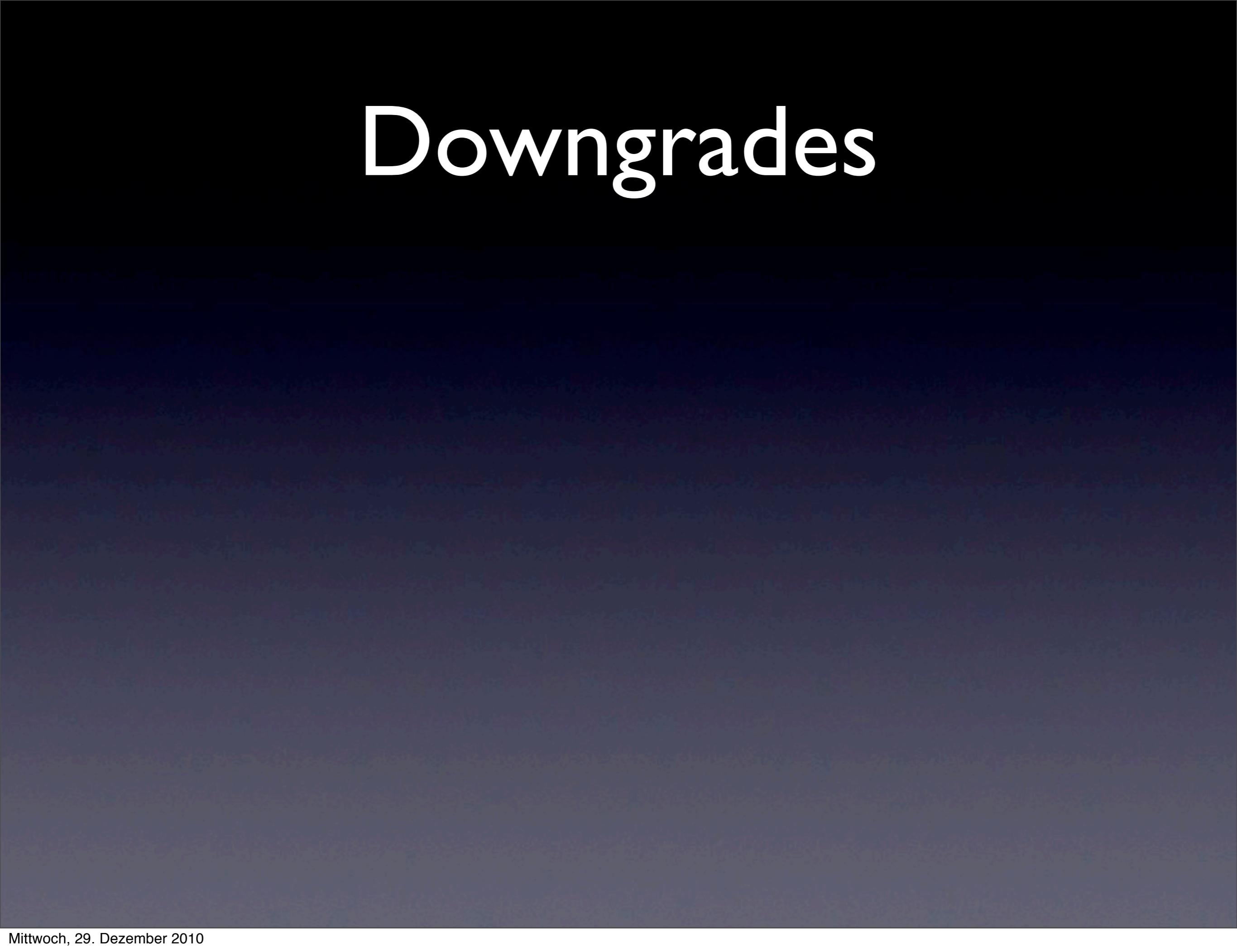
- The hypervisor does not enforce LV2 and game integrity
- You can just patch LV2 to run games from HDD

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		
Encrypted storage		✓		BYPASSED
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	✓
User/kernelmode				✓
Anti-downgrade eFUSES			✓	

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		
Encrypted storage		✓		BYPASSED
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	USELESS
User/kernelmode				✓
Anti-downgrade eFUSES			✓	

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		
Encrypted storage		✓		BYPASSED
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	USELESS
User/kernelmode				✓
Anti-downgrade eFUSES			✓	

# Downgrades



# Downgrades

- Sony fixed the exploit

# Downgrades

- Sony fixed the exploit
- Service mode triggered by USB “JIG”
- HMAC authenticated, keys dumped

# Downgrades

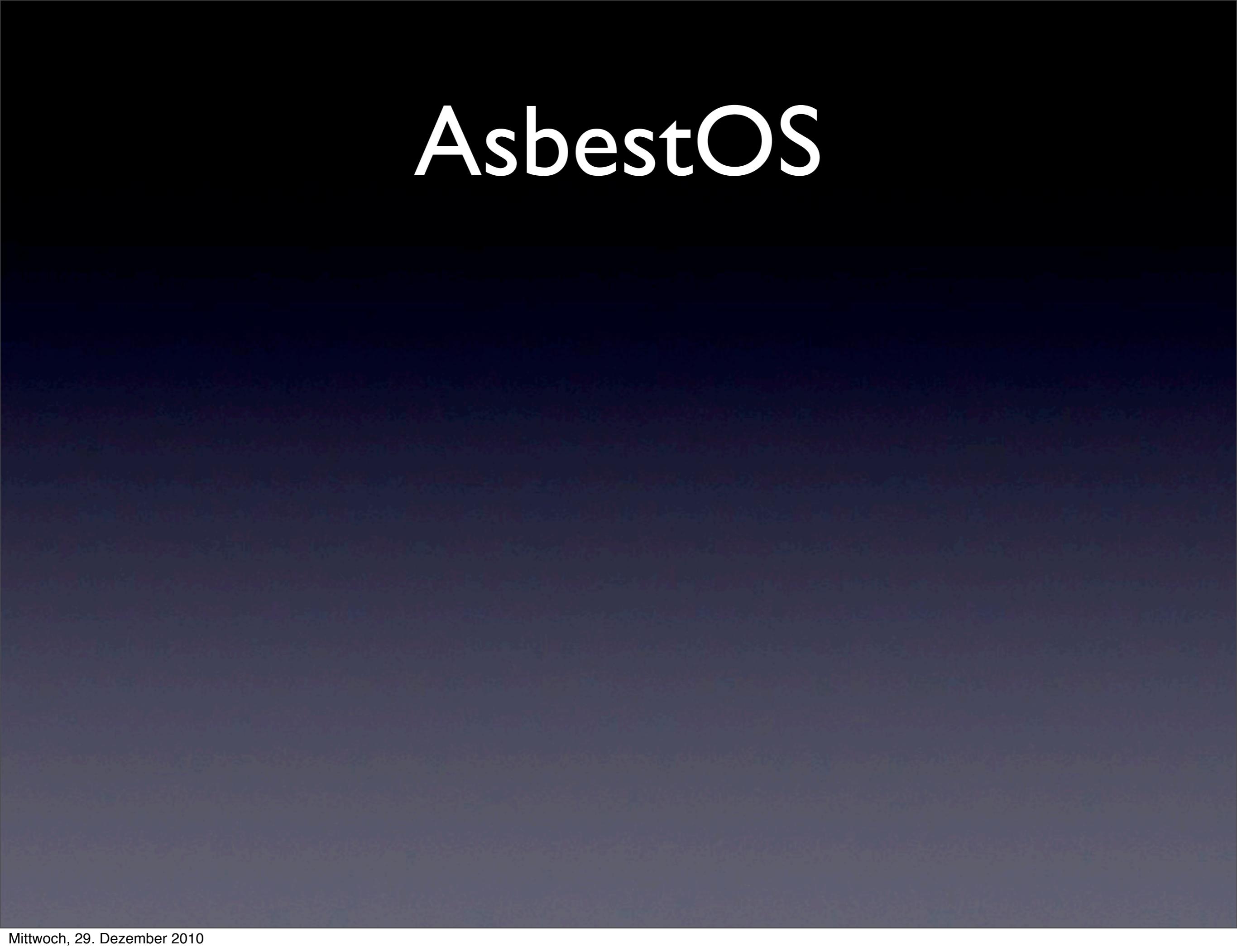
- Sony fixed the exploit
- Service mode triggered by USB “JIG”
  - HMAC authenticated, keys dumped
- Leaked service app used to enable downgrades



You have earned a trophy.  
More Piracy

- Sony fixed the exploit
- Service mode triggered by USB “JIG”
  - HMAC authenticated, keys dumped
- Leaked service app used to enable downgrades

# AsbestOS



# AsbestOS

- Replace LV2/GameOS in memory

# AsbestOS

- Replace LV2/GameOS in memory
- OtherOS mode and GameOS mode are virtually identical
- Except GameOS can do more stuff, e.g. 3D

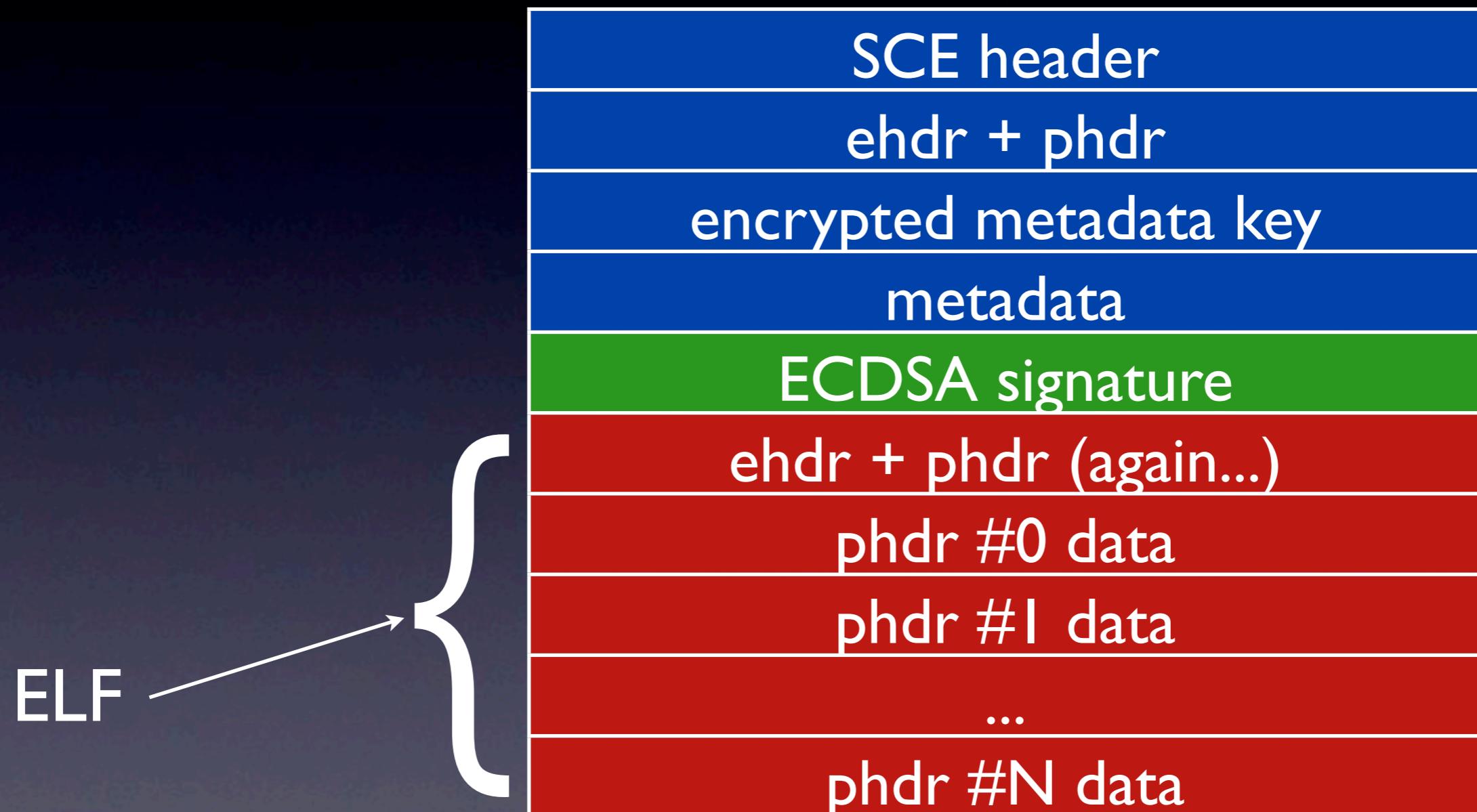
# AsbestOS

- Replace LV2/GameOS in memory
- OtherOS mode and GameOS mode are virtually identical
  - Except GameOS can do more stuff, e.g. 3D
- Run Linux again (even on the Slim!)

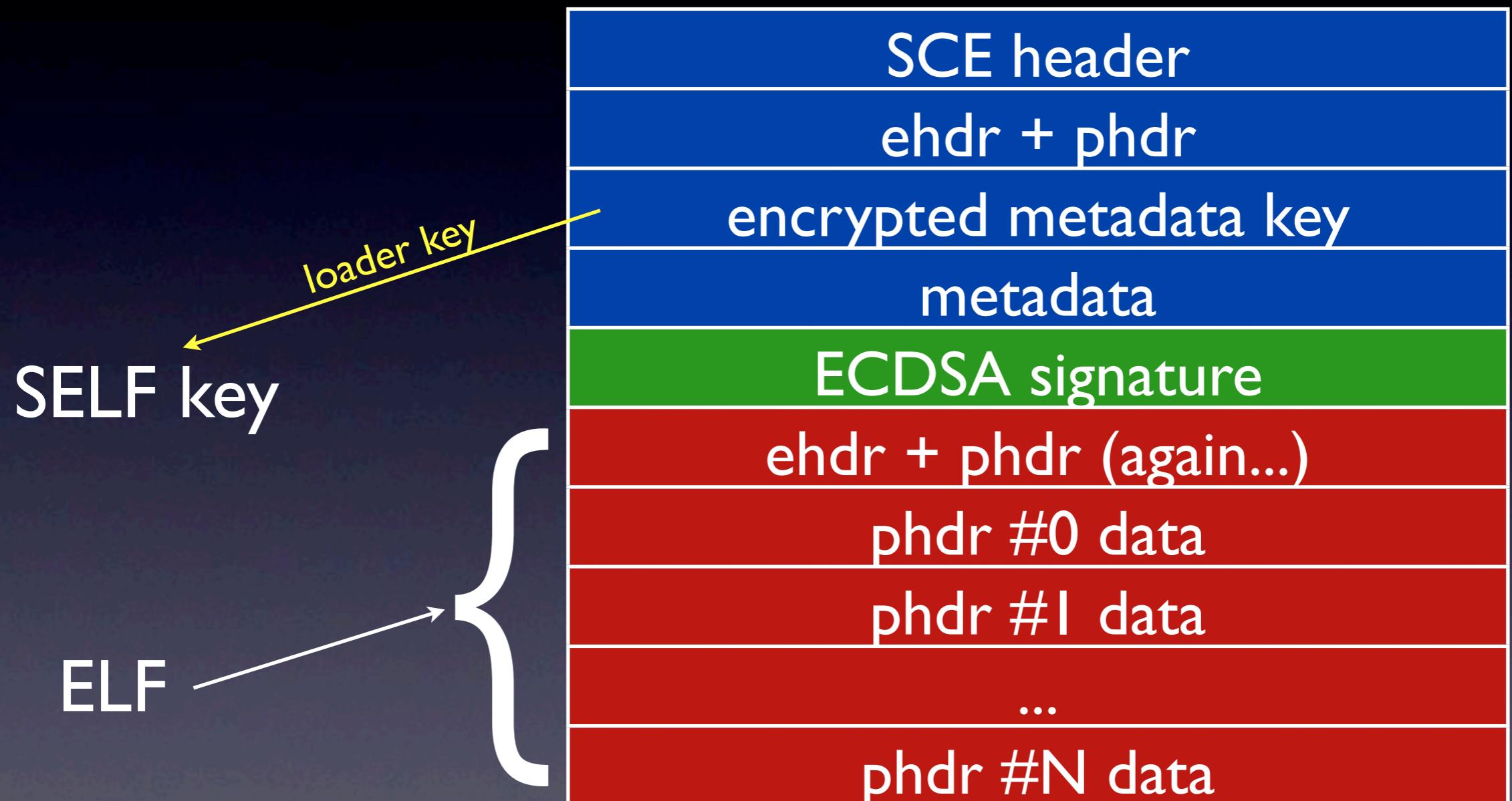
# AsbestOS

- Replace LV2/GameOS in memory
- OtherOS mode and GameOS mode are virtually identical
  - Except GameOS can do more stuff, e.g. 3D
- Run Linux again (even on the Slim!)
- Use NetRPC to remote-control the PS3 and experiment...

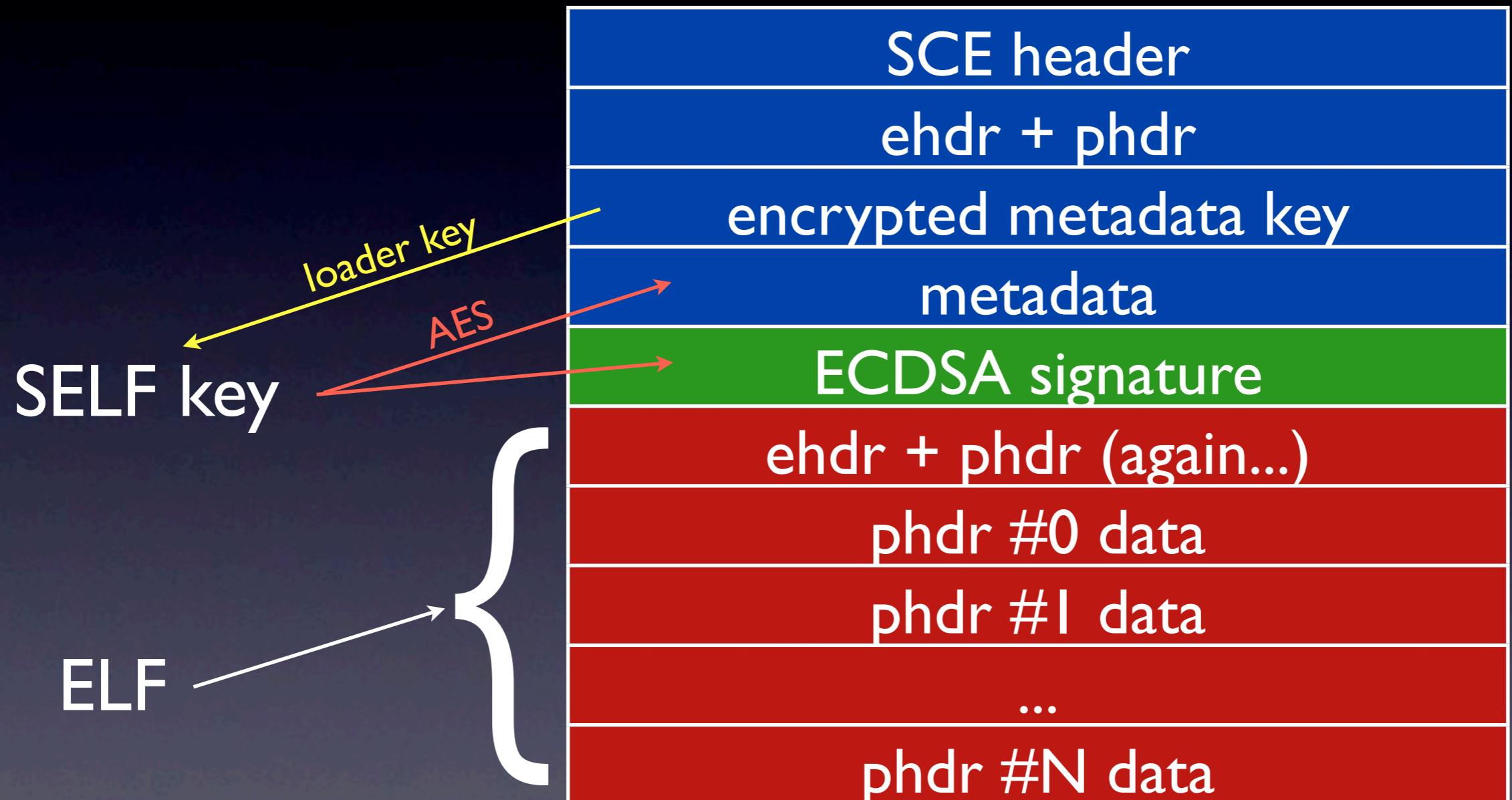
# SELFs



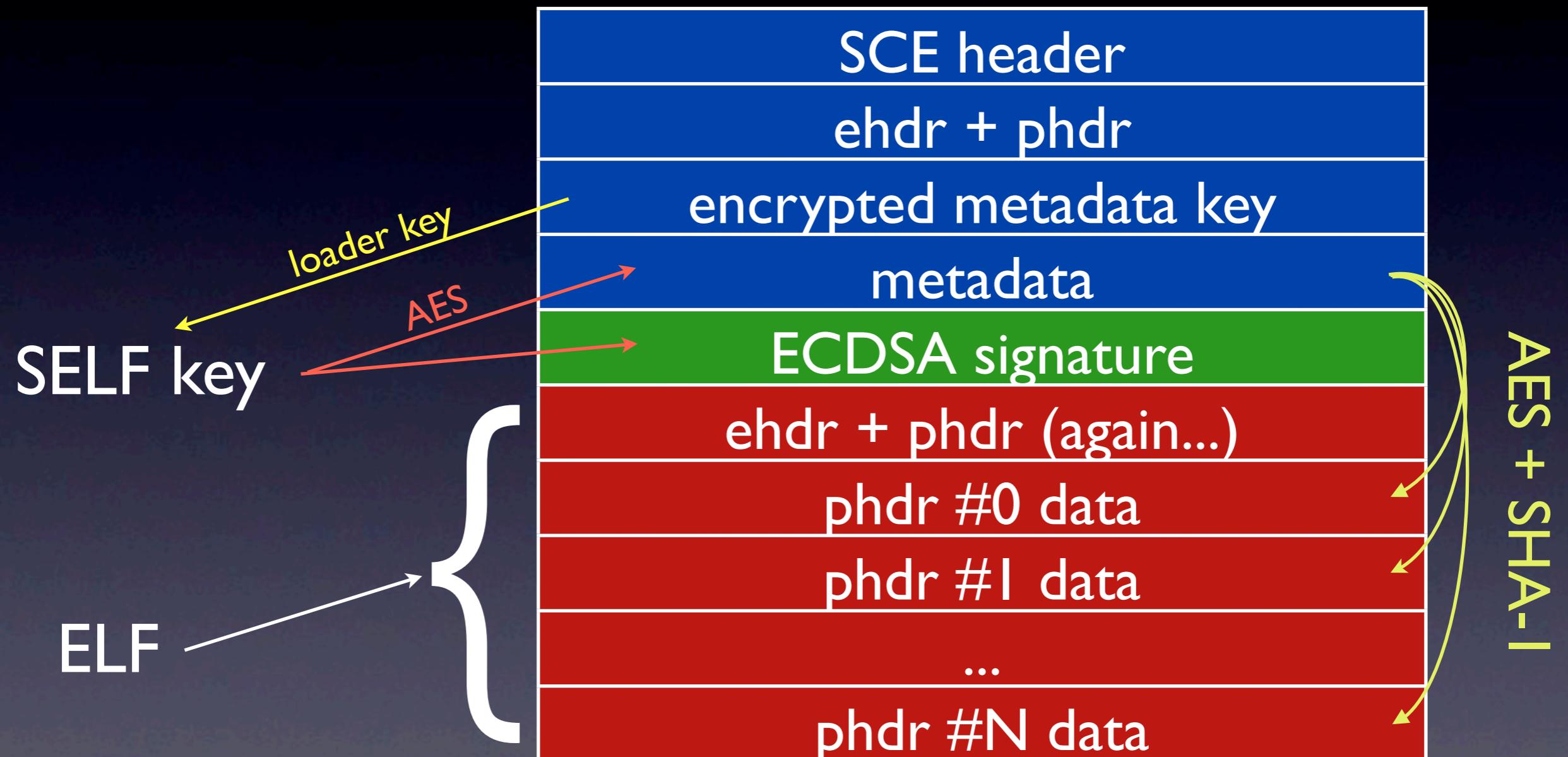
# SELFs



# SELFs

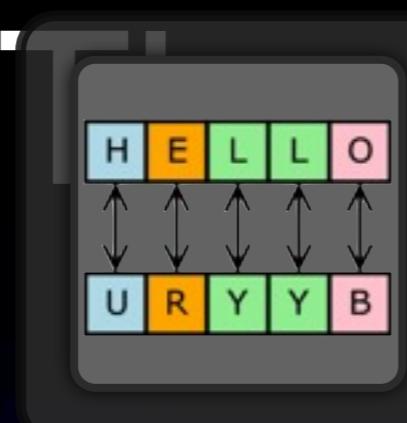


# SELFs



# The Oracle

- Sony's idea: "No one can see our code!"
- ... unless the PPE is compromised
- Decrypting all code possible from GameOS
  - security coprocessor pointless!
- But we want keys!



Oracle

You have earned a trophy.  
🏆 Obfuscation useless

- Sony's idea: "No one can see our code!"
- ... unless the PPE is compromised
- Decrypting all code possible from GameOS
  - security coprocessor pointless!
- But we want keys!

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓		✓	✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		
Encrypted storage		✓		BYPASSED
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	USELESS
User/kernelmode				✓
Anti-downgrade eFUSES			✓	

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓			✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		
Encrypted storage		✓		
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	
User/kernelmode				✓
Anti-downgrade eFUSES			✓	

INEFFECTIVE  
POINTLESS

BYPASSED

USELESS

# Chain of Trust

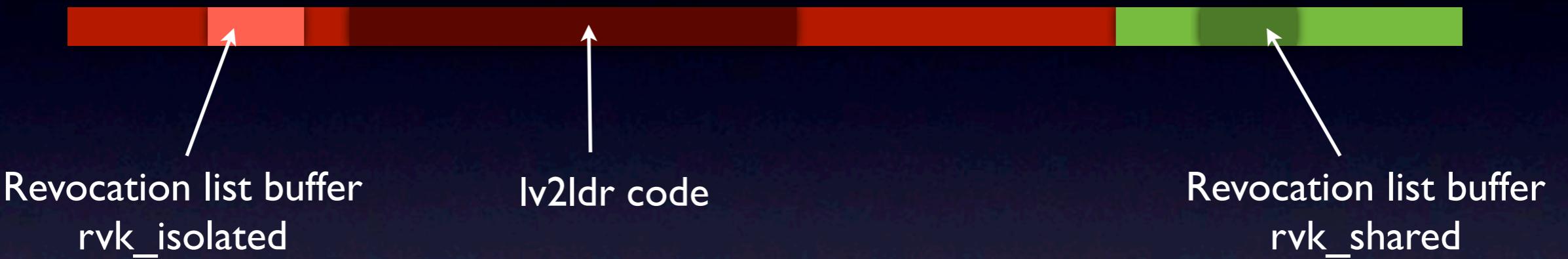
Name	Processor / Mode	updateable	revocable*	usage
bootldr	SPE	✗	✗	boot lv0
lv0	PPE HV	✓	✗	boot lv1
metldr	SPE	✗	✗	run *ldr
lv1ldr	SPE	✓	✗	decrypt lv1
lv1	PPE HV	✓	✗	hypervisor
isoldr	SPE	✓	✗	decrypt modules
sc_iso	SPE	✓	✓	
...				
lv2ldr	SPE	✓	✗	decrypt lv2
lv2	PPE SV	✓	✓	kernel
appldr	SPE	✓	✓	decrypt games
some game	PPE PS	✓	✓	:-)

# Chain of Trust

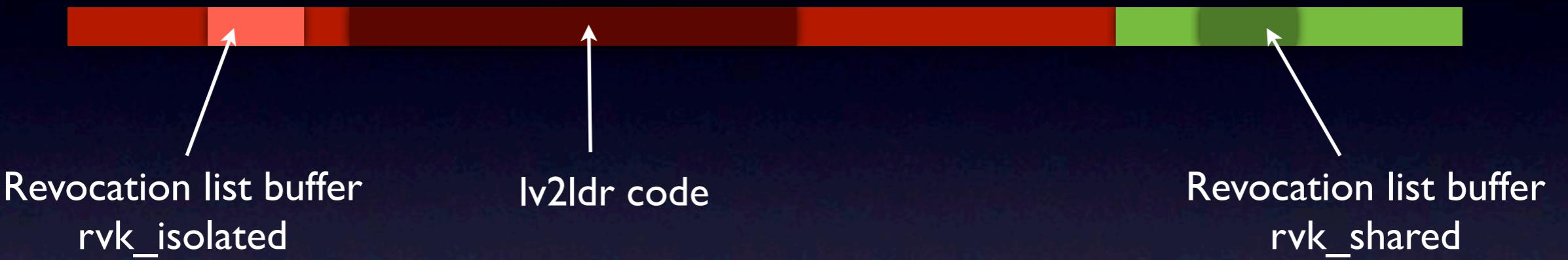
Name	Processor / Mode	updateable	revocable*	usage
bootldr	SPE	✗	✗	boot lv0
lv0	PPE HV	✓	✗	boot lv1
metldr	SPE	✗	✗	run *ldr
lv1ldr	SPE	✓	✗	decrypt lv1
lv1	PPE HV	✓	✗	hypervisor
isoldr	SPE	✓	✗	decrypt modules
sc_iso	SPE	✓	✓	
...				
lv2ldr	SPE	✓	✗	decrypt lv2
lv2	PPE SV	✓	✓	kernel
appldr	SPE	✓	✓	decrypt games
some game	PPE PS	✓	✓	:-)

\*as per Sony's specification

# Breaking loaders

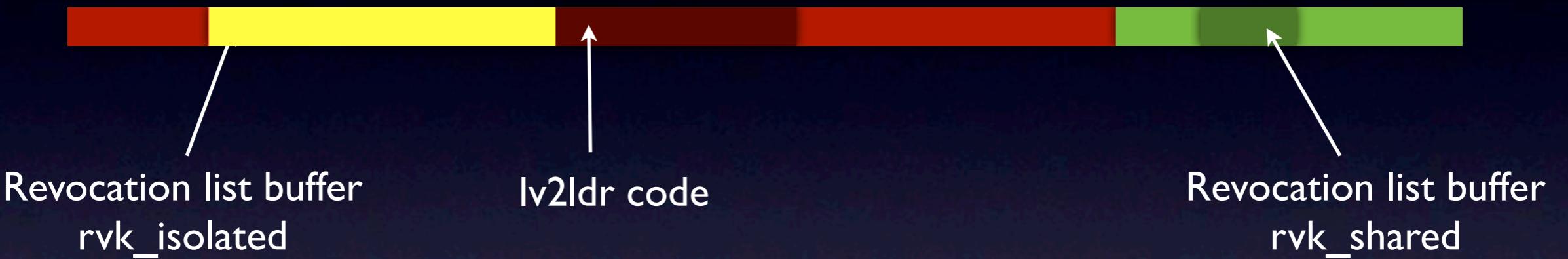


# Breaking loaders



```
memcpy(rvk_isolated, rvk_shared, *((int *) (rvk_shared + 0x1c)))
```

# Breaking loaders

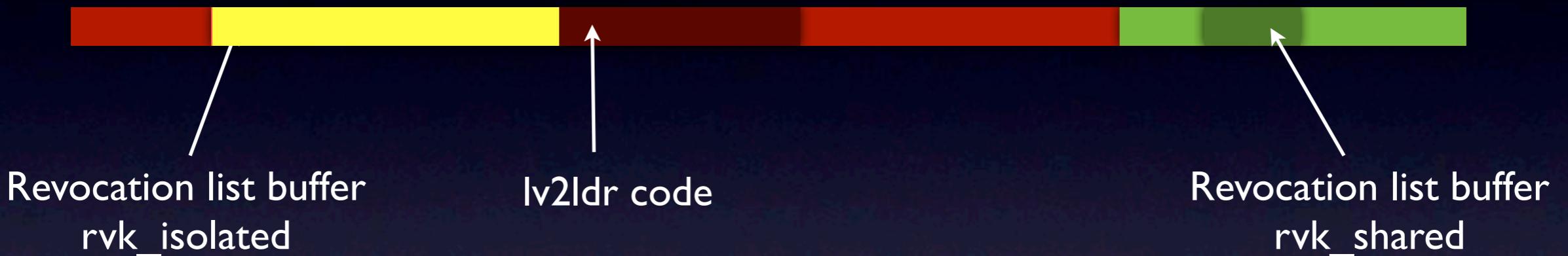


```
memcpy(rvk_isolated, rvk_shared, *((int *) (rvk_shared + 0x1c)))
```

# Bre

6692d179032205  
82592e77a204a8  
1b91b9b73c68f9  
b3b9accda43860  
2901308bbd685c  
672f11cedf36c5  
07ebd2779e3e71  
1d6b501ae0f003

You have earned a trophy.  
Obtained AES keys



```
memcpy(rvk_isolated, rvk_shared, *((int *) (rvk_shared + 0x1c)))
```

- „Only“ a bug in isolated loaders
- Chain of Trust already broken for all sold consoles now.



You have earned a trophy.  
🏆 Chain of Fail

- „Only“ a bug in isolated loaders
- Chain of Trust already broken for all sold consoles now.
- This is Fail™. But it's not Epic™ yet...

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓			✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		
Encrypted storage		✓		
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	
User/kernelmode				✓
Anti-downgrade eFUSES			✓	

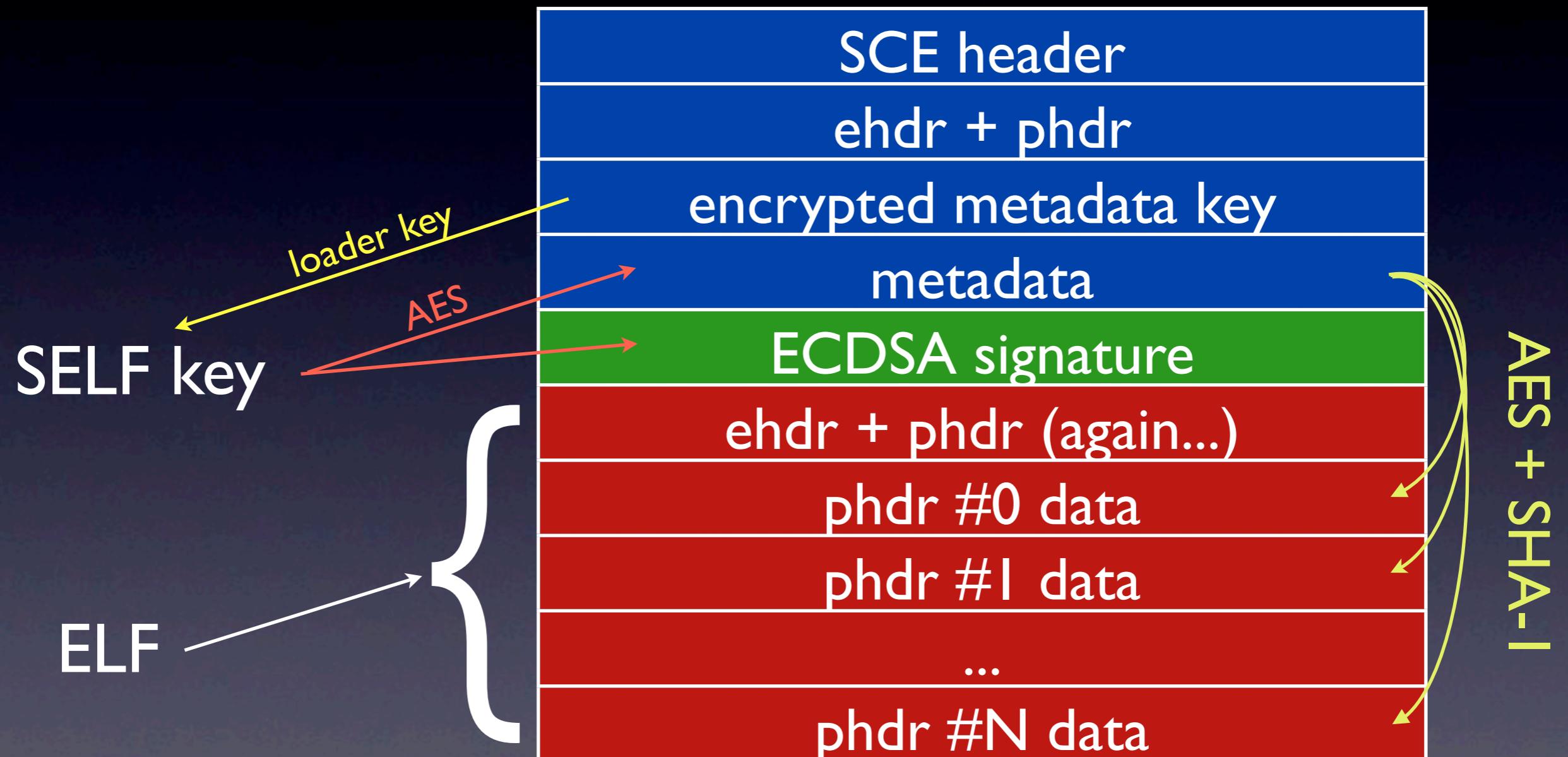
INEFFECTIVE  
POINTLESS

BYPASSED

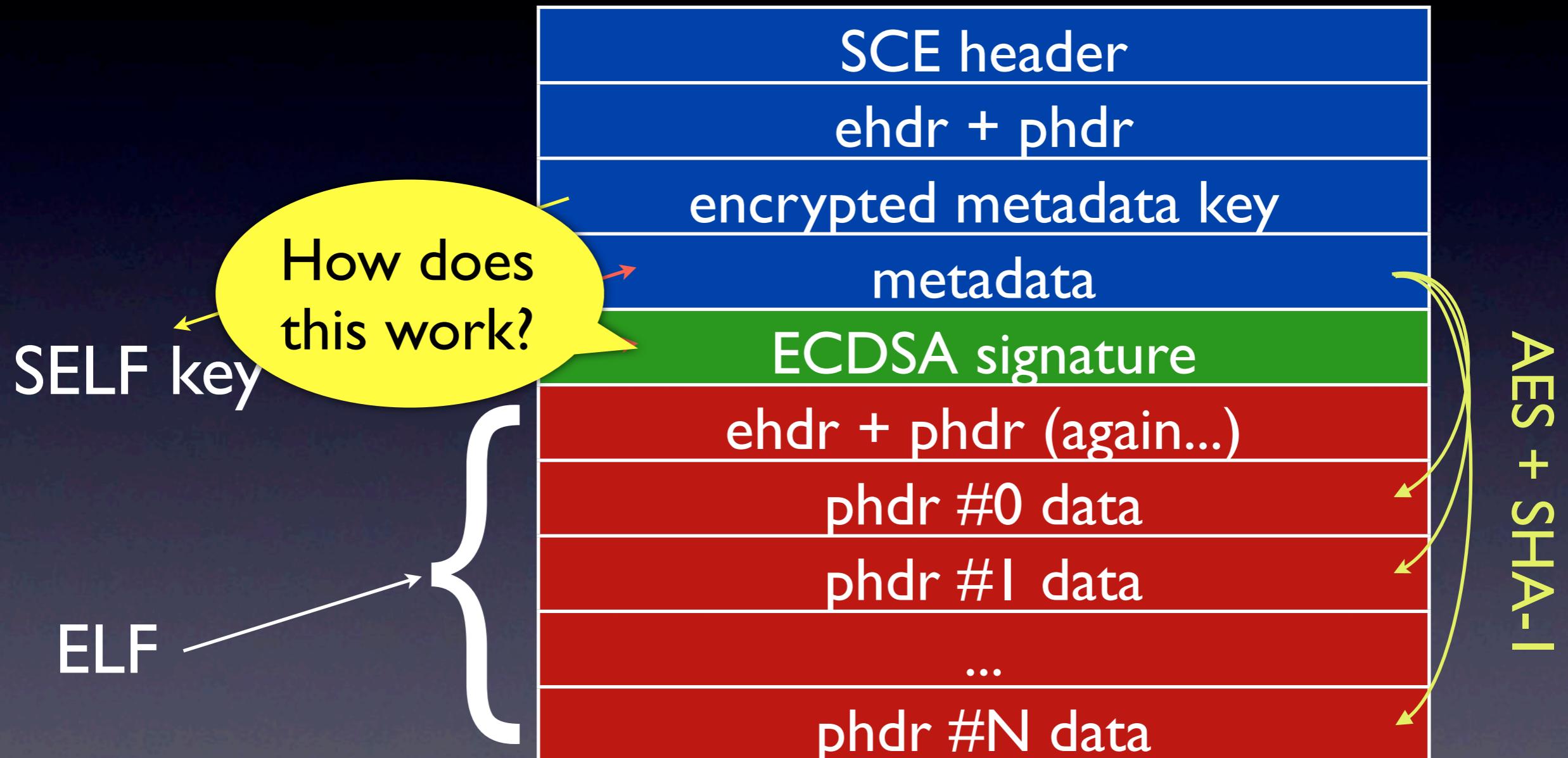
USELESS

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	BROKEN
Per-console keys		✓	✓	✓
Signed executables	✓			INEFFECTIVE
Security coprocessor		✓		POINTLESS
Full media encryption and signing		✓		
Encrypted storage		✓		BYPASSED
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	USELESS
User/kernelmode				✓
Anti-downgrade eFUSES			✓	

# SELFs



# SELFs



# ECDSA

These are public:

$p, a, b, G, N$  (elliptic curve params)

$Q$  = public key

$e$  = hash of data

$R, S$  = signature,

and these are private:

$m$  = random

$k$  = private key.

A signature is a pair of numbers  $R, S$  computed by the signer as

$$R = (mG)_x$$

$$S = \frac{e + kR}{m}.$$

It is imperative to have a random  $m$  for every signature: from a pair of signatures that use the same  $m$ , we can compute  $m$  and  $k$ .

$$R = (mG)_x \quad R = (mG)_x$$

$$S_1 = \frac{e_1 + kR}{m} \quad S_2 = \frac{e_2 + kR}{m}$$

When  $m$  is identical for two signatures, so is  $R$ , and

$$S_1 - S_2 = \frac{e_1 - e_2}{m}$$

$$m = \frac{e_1 - e_2}{S_1 - S_2}$$

$$k = \frac{mS_i - e_i}{R} \quad \left[ = \frac{e_1S_2 - e_2S_1}{R(S_1 - S_2)} \right].$$

# Our ECDSA code

Used for HBC's network update function

```
def generate_ecdsa(k, sha):
    k = bytes_to_long(k)
    e = bytes_to_long(sha)

    m = open("/dev/random", "rb").read(30)

    if len(m) != 30:
        raise Exception("Failed to get m")
    m = bytes_to_long(m) % ec_N

    r = (m * ec_G).x.tobignum() % ec_N
    kk = ((r * k) + e) % ec_N
    s = (bn_inv(m, ec_N) * kk) % ec_N
    r = long_to_bytes(r, 30)
    s = long_to_bytes(s, 30)
    return r,s
```

# Our ECDSA code

Used for HBC's network update function

```
def generate_ecdsa(k, sha):
    k = bytes_to_long(k)
    e = bytes_to_long(sha)

    m = open("/dev/random", "rb").read(30)

    if len(m) != 30:
        raise Exception("Failed to get m")
    m = bytes_to_long(m) % ec_N

    r = (m * ec_G).x.tobignum() % ec_N
    kk = ((r * k) + e) % ec_N
    s = (bn_inv(m, ec_N) * kk) % ec_N
    r = long_to_bytes(r, 30)
    s = long_to_bytes(s, 30)
    return r,s
```

# Sony's ECDSA code

```
int getRandomNumber()
{
    return 4; // chosen by fair dice roll.
              // guaranteed to be random.
}
```

With private keys you can  
SIGN THINGS



You have earned a trophy.  
🏆 Public Private Keys

With private keys you can  
**SIGN THINGS**

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	BROKEN
Per-console keys		✓	✓	✓
Signed executables	✓			INEFFECTIVE
Security coprocessor		✓		POINTLESS
Full media encryption and signing		✓		
Encrypted storage		✓		BYPASSED
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	USELESS
User/kernelmode				✓
Anti-downgrade eFUSES			✓	

	Xbox	Wii	360	PS3
On-die bootROM	✓	✓	✓	✓
On-die key storage		✓	✓	
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓			✓
Security coprocessor		✓		✓
Full media encryption and signing		✓		
Encrypted storage		✓		✓
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	✓
User/kernelmode				✓
Anti-downgrade eFUSES			✓	

Annotations in red text:

- EPIC FAIL BROKEN (overlaid on the 360 and PS3 columns for Public-key crypto, Chain of trust, and Security coprocessor)
- INEFFECTIVE POINTLESS (overlaid on the 360 and PS3 columns for Signed executables, Security coprocessor, and Full media encryption and signing)
- BYPASSED (overlaid on the 360 and PS3 columns for Encrypted storage)
- USELESS (overlaid on the 360 and PS3 columns for Hypervisor)



You have earned a trophy.

**Fail0verflow**

	Xbox	Wii	360	PS3
On-die keys	✓	✓	✓	✓
Public-key crypto	✓	✓	✓	✓
Chain of trust	✓		✓	✓
Per-console keys		✓	✓	✓
Signed executables	✓			✓
Security coprocessor		✓	✓	✓
Full media encryption and signing		✓	✓	✓
Encrypted storage		✓	✓	
Self-signed storage		✓		
Memory encryption/hashing			✓	
Hypervisor			✓	✓
User/kernelmode				✓
Anti-downgrade eFUSES			✓	

Annotations in red text:

- EPIC FAIL BROKEN (overlaid on the PS3 column)
- INEFFECTIVE POINTLESS (overlaid on the PS3 column)
- BYPASSED (overlaid on the PS3 column)
- USELESS (overlaid on the PS3 column)

# Thanks, Sony!



<http://fail0verflow.com>