

Try Harder 2 Hardening the COREs



Shawn C

#whois

- * Shawn C[a.k.a "citypw"]
- * Day job at TYA infotech
 - * Open source security consulting
- * GNU/Linux security engineer
- * Free/libre SW/FW/HW enthusiasts
- * Member of EFF/FSF/FSFE/SFC
- * Patient Zer0 at Hardenedlinux community(<https://hardenedlinux.github.io/>)



#cat /proc/agenda

- * History: Ring 3
- * Attacking the core
- * Under the water
- * Invincible devil
- * Hope or delusion?

#Ring 3

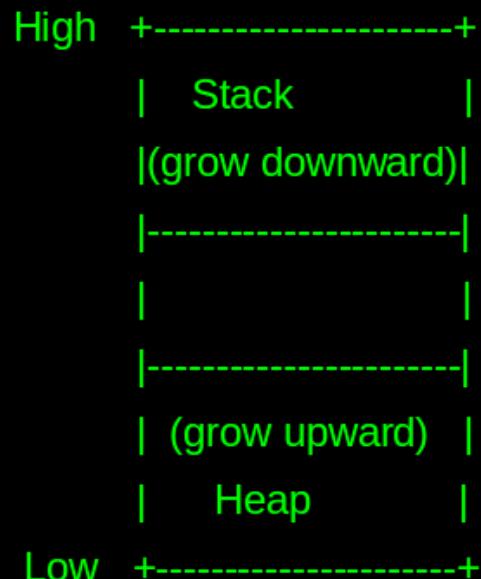
- * MAC/DAC/Sandboxing(seccomp)
- * Baseline checks(STIG-4-Debian)
- * Firewall/IDS/SOC
- * etc

#We had a history with Ring 3

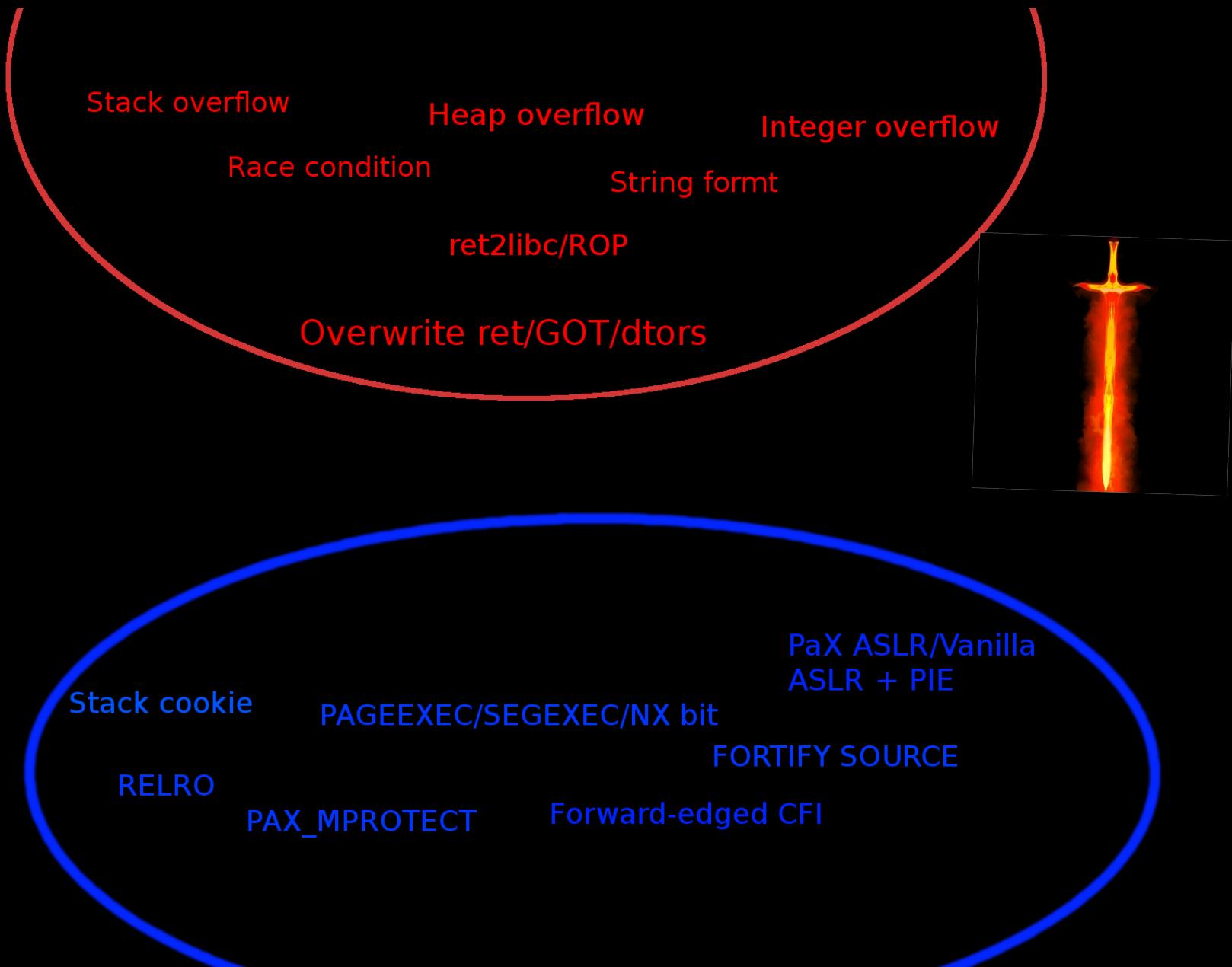
* Once upon a time, the stack was so "pure"...



- * Stack/Heap layout
- * Stack grows down (x86, MIPS)
- * ESP points to the current top of the stack
- * EBP points to the current function frame



#War at Ring 3



#End of story?

We got everything we need! Ok, this is it.
Thanks for coming. Bye, cruel world!

#Why attack the core?

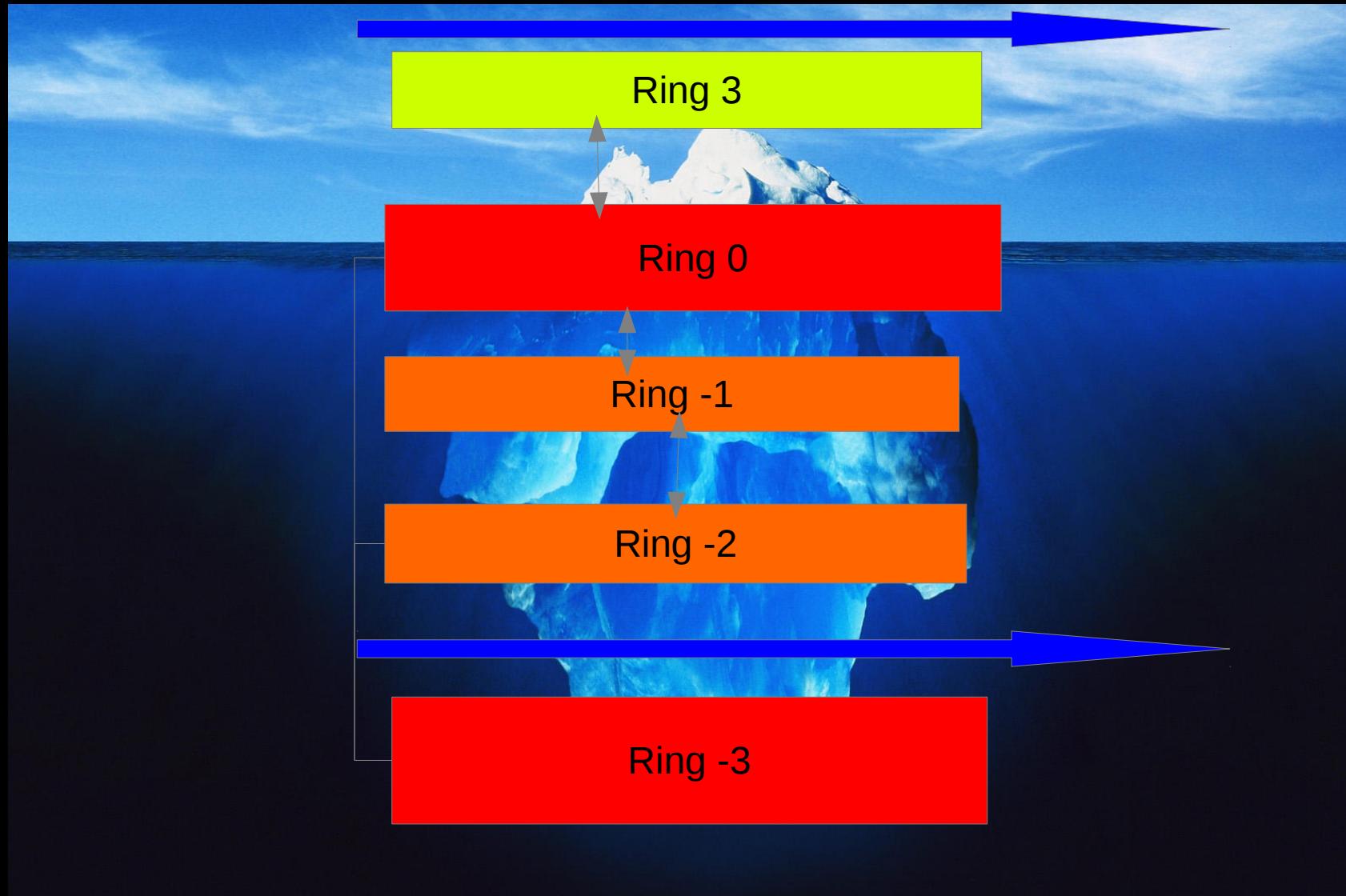
- * Linux kernel sucks in 2000s
 - * One null-ptr deref can rule them all
- * Still a cargo-cult security in 2017?
- * Harder to exploit userspace programs

#Defend the core



#Wait, which CORE exactly?

* RING 0 is **not** the CORE anymore



#Under the water

- * VM guest escape
- * Did all device drivers follow the best practice(let's say IOMMU)?
- * Old/new good/bad attacks on SMM
- * Persistent attack chain
 - * -1: Hijacking the kernel(perf impact?)
 - * -2: Memory tricks

See the reference...

#Demo

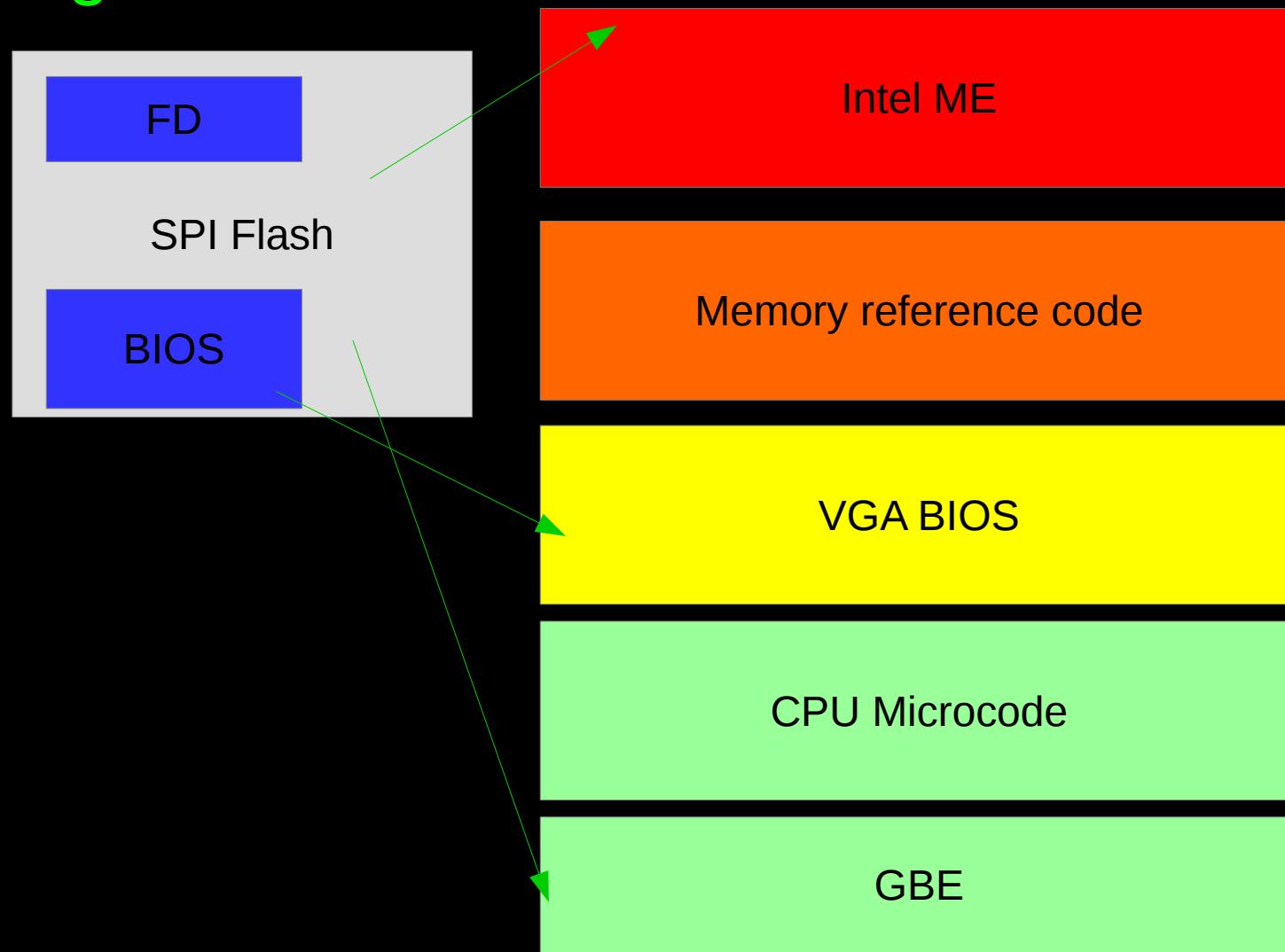
What could possibly go wrong with your
“trusted” watcher? Don’t freaking out...

#Invincible devil

- * Intel ME
- * A lot of ME "apps" based on it
- * Changed a lot since v11
- * Can't be disabled

#From a libre FW's perspective

* Not good



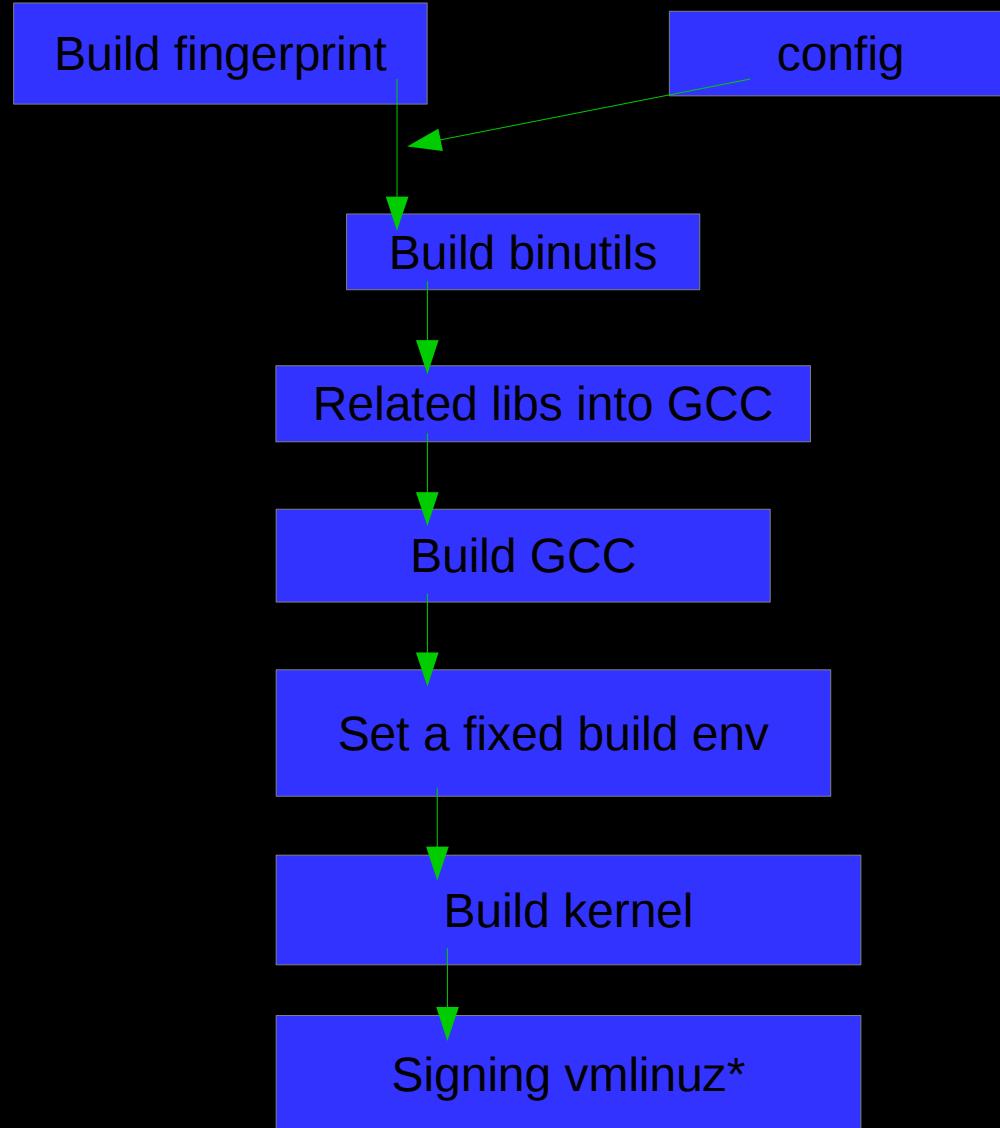
#Hope or delusion?

- * Some trade-off must be made
- * Reproducible builds for PaX/Grsecurity
- * Hardenedboot: Measured boot & verified boot
- * Restricted ME via minimizing its functions

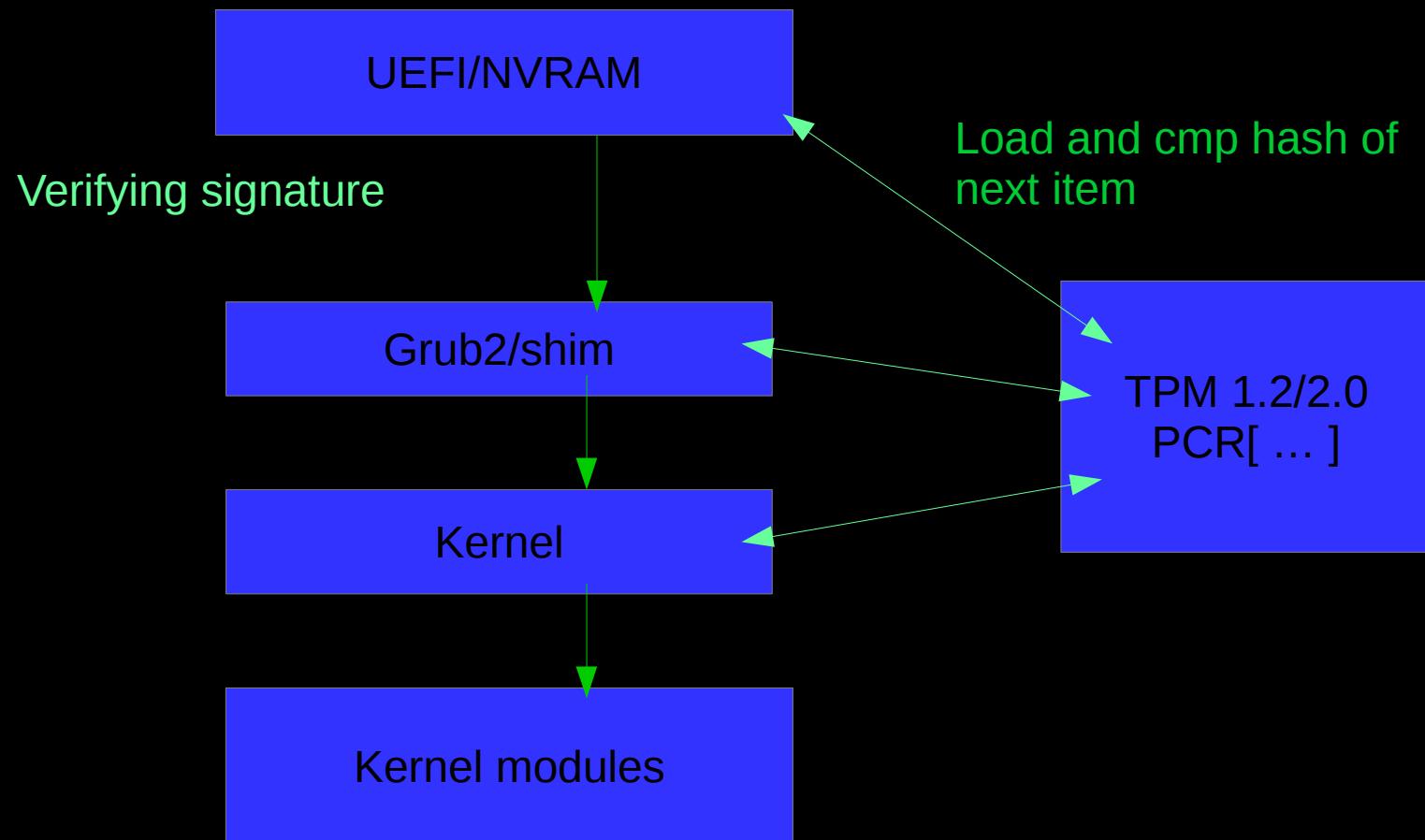
#Why PaX/Grsecurity matters

- * Kill bug classes
- * Kill exploit vectors
- * Assumption: Let data center takes physical security into account
 - * Kernel is still the path to the under water
 - * Hardened guards kills the attack surfaces

#Reproducible builds for PaX/Grsecurity



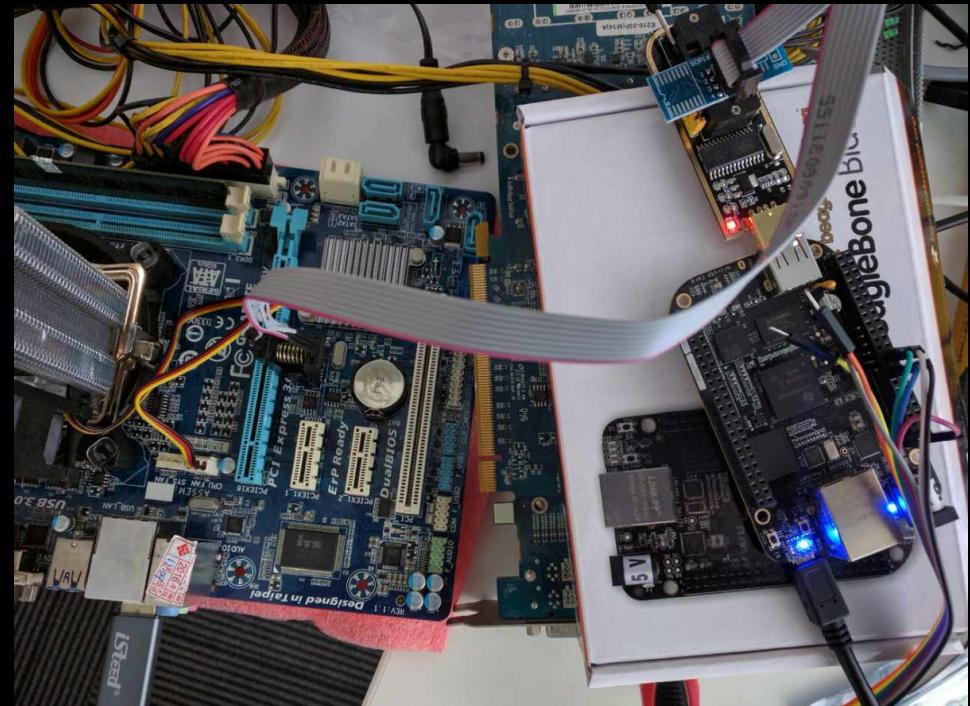
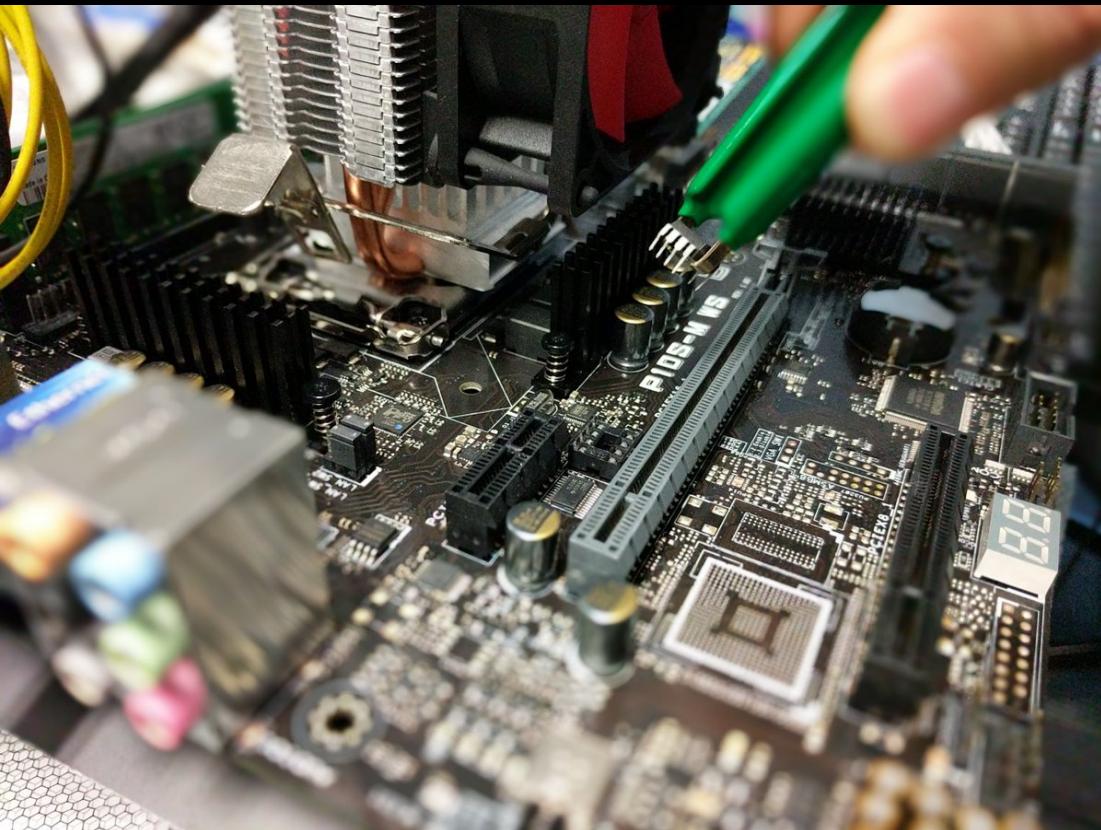
#Hardened Boot



#Free/libre solution?

- * Coreboot/FSP
- * Libreboot
- * Situational hardening
 - * Old good machines for critical assets
 - * Newer machines for generic purposes
- * Reference model for custom firmware

#Neutralizing ME



Mainboard	CPU	Tested BIOS
GA-B75M-D3H	SandyBridge	OEM/Coreboot
GA-B75M-D3V	IvyBridge	OEM/Coreboot
Lenovo T420	IvyBridge	OEM/Coreboot
Lenovo X220/X220i	SandyBridge	OEM/Coreboot
Lenovo X230	IvyBridge	OEM/Coreboot
Chromebook XE550C22	IvyBridge	OEM/Coreboot
ASUS P10S-M WS	Skylake	OEM

#Extra notes;-)

- * Neutralized ME affected remote attestation via SGX?
- * Think harder about your situational hardening solution before ask OEM write your pk
- * You don't need Intel Bootguard if the data center could take care of physical security
- * Big clouds(AWS/Google/Facebook/BAT3H/etc) should do the situational hardening for their core infrastructure. Otherwise it might become someone else's computer;-)
- * Masters of Pwn killed by PaX/Grsecurity

#Are we done?

- * Or just another starting point?
- * Know your enemy(from Ring 3/0/-1/-2/-3)
- * Risk assessment for important production/assets
 - * Known vulnerability/exploit vectors

**HardenedLinux's
roadmap**



The West Of
Middle Earth
At The End Of
The Third Age

Crypto
Engineering

ARTHEDAIN

Firmware

ERIADOR

MINHIRIATH

Compiler

ENEDWAITH

Situational
Hardening

FORODWAITH

Angmar
Mount Gunduband

Ered Mithrin

Iron Hills

HITHAEGLIR

Ettenmoors

Weather Hills

Rhudaur

KERNEL

Old Forest

The Shire

Bree

Rivendell

Eregion

Dunland

Tsengard

Lorien

Fangorn

Helms Deep

N. Ithilien

Anfalas

Lebennin

S. Ithilien

Free/libre & Open
Source Software's eco-
system!

* GPL-compliance
* Legislation
* Education

RHOGLYON

The Brown Lands

Ered Lithui (Ash Mountains)

Plateau of Gorgoroth

MORDOR

NURN

Adversary

Reference

* PaX/Grsecurity:

<https://grsecurity.net/>

* Coreboot:

<http://coreboot.org/>

* Linux kernel mitigation checklist:

https://hardenedlinux.github.io/system-security/2016/12/13/kernel_mitigation_checklist.html

* Ring 0: Linux kernel vulnerability & exploitation & silent fixes

https://github.com/hardenedlinux/grsecurity-101-tutorials/blob/master/kernel_vuln_exp.md

* Virtualization security:

https://github.com/hardenedlinux/grsecurity-101-tutorials/blob/master/virt_security.md

Reference

* Firmware security:

https://github.com/hardenedlinux/firmware-anatomy/blob/master/hack_ME/firmware_security.md

* Reproducible builds for PaX/Grsecurity

<https://github.com/hardenedlinux/grsecurity-reproducible-build>

* Hardened Boot:

https://github.com/hardenedlinux/Debian-GNU-Linux-Profiles/tree/master/docs/hardened_boot

* Neutralized ME with coreboot stuff

https://github.com/hardenedlinux/hardenedlinux_profiles/tree/master/coreboot

* Intel ME's info:

https://github.com/hardenedlinux/firmware-anatomy/blob/master/hack_ME/me_info.md

QA

Thanks