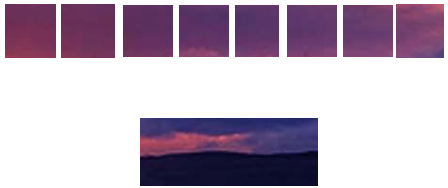
资源代价与安全算力

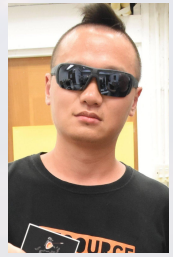
开放基础架构安全防护:对抗复杂性

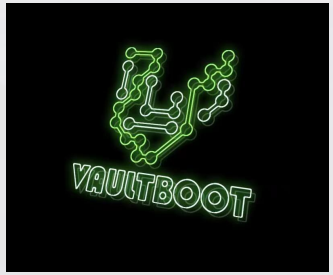
HARDENED VAULT
Shawn Chang



#whois

- Shawn Chang [a.k.a “citypw”]
- 赛博堡垒有限公司（HardenedVault Limited）CEO
- HardenedLinux社区创始人
- 12年开源基础架构安全经验
- 密码朋克
- 自由软件/固件/硬件狂热玩家
- 塔防/纵深防御实践者



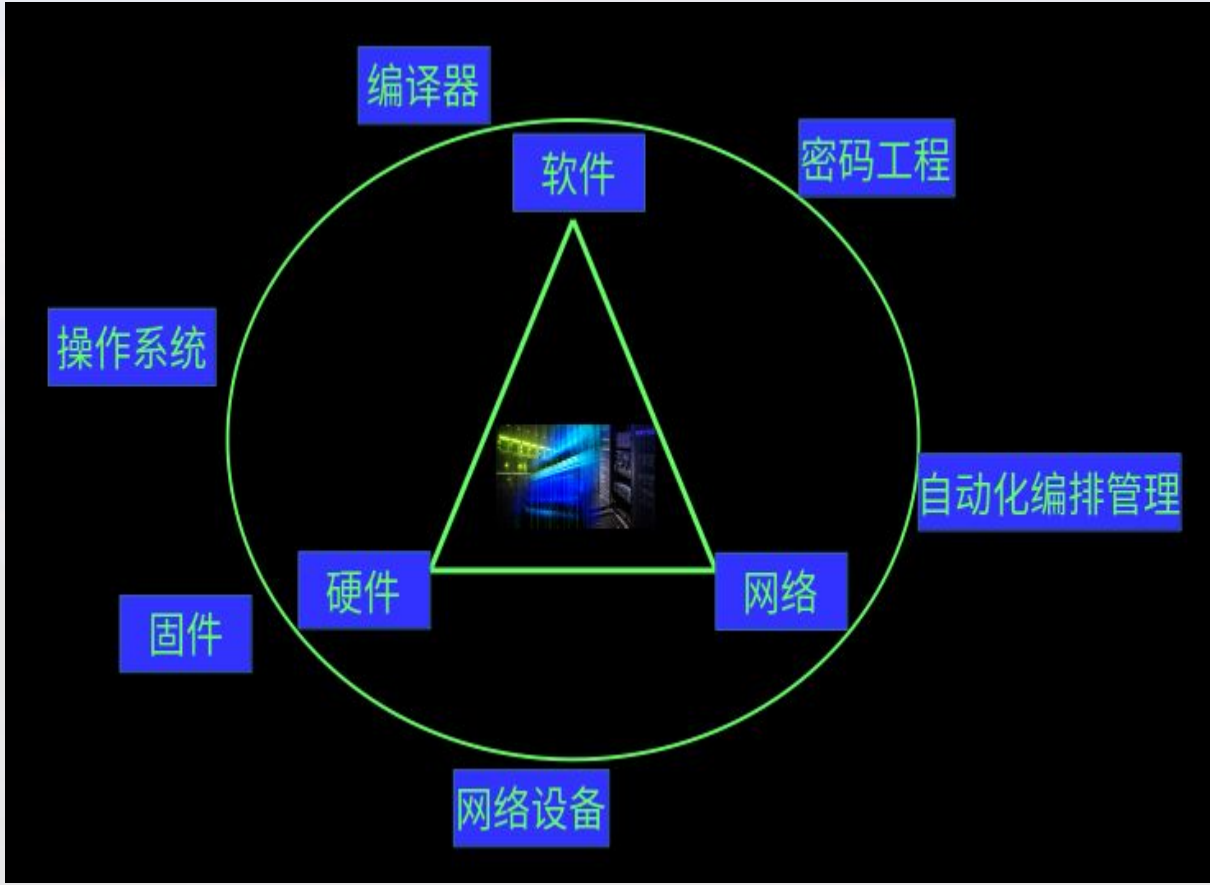


01 基础架构安全

高级威胁防护背景

核心基础架构定义


debian
Software Analyzers
GnuPG
OpenSSH
OpenSSL
Cryptography and SSL/TLS Toolkit
The Fuzzing Project


编译器
软件
密码工程
操作系统
自动化编排管理
硬件
网络
固件
网络设备

高级威胁趋势

A deep dive into an NSO zero-click iMessage exploit: Remote Code Execution

Posted by Ian Beer & Samuel Groß of Google Project Zero

We want to thank Citizen Lab for sharing a sample of the FORCEDENTRY exploit with us, and Apple's Security Engineering and Architecture (SEAR) group for collaborating with us on the technical analysis. The editorial opinions reflected below are solely Project Zero's and do not necessarily reflect those of the organizations we collaborated with during this research.

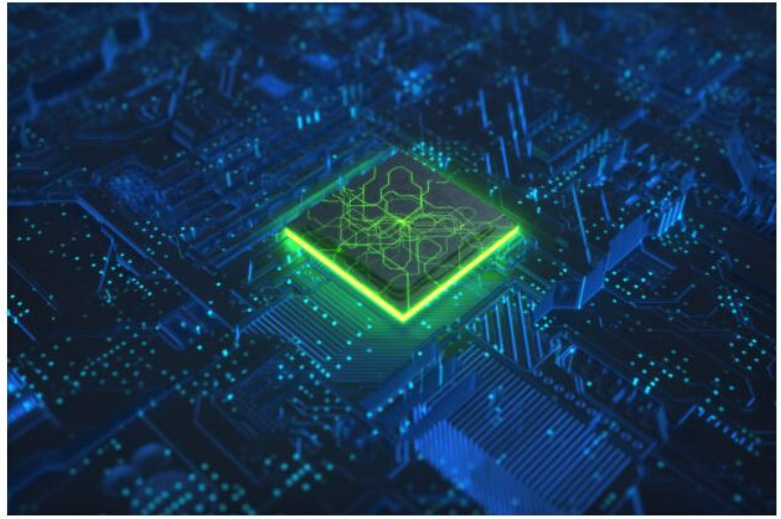
Earlier this year, Citizen Lab managed to capture an NSO iMessage-based zero-click exploit being used to target a Saudi activist. In this two-part blog post series we will describe for the first time how an in-the-wild zero-click iMessage exploit works.

Based on our research and findings, we assess this to be one of the most technically sophisticated exploits we've ever seen, further demonstrating that the capabilities NSO provides rival those previously thought to be accessible to only a handful of nation states.

The vulnerability discussed in this blog post was fixed on September 13, 2021 in iOS 14.8 as CVE-2021-30860.

HP iLO and the Newly Discovered iLOBleed Rootkit

December 29, 2021 By Josh Stuifbergen



Iranian researchers at Amnpardaz security firm have discovered rootkits in HPs iLO (Integrated Lights-Out) management modules. These optional chips are added to servers for remote management and grant full high-level access to the system. This includes the ability to turn the server on and off, configure hardware and firmware settings, and additional administrator functions. The rootkit name, iLOBleed, is based on the malware module *Implant.ARM.iLOBleed.a* discovered in the iLO firmware. This is the first known discovery of an iLO rootkit.

高级威胁防护趋势

*欧盟委员会资助的地平线2020计划中加大针对硬件，固件，操作系统等基础安全领域的研发投入。

*欧盟成员国独立的专业领域funding：可信计算，固件安全等。

* 下一代6G通信合规会要求具备高级防御的节点数大幅度提升。

ERICSSON NOKIA

* “80%的企业在过去2年中至少遭遇过一次固件级别的攻击，但这些企业中只有29%的具有定向的固件经费。”--- 微软报告，2021年3月

Microsoft

* 美国国防部CISA于2021年5月宣布VBOS(Vulnerabilities Below the Operating System)计划，要求机构必须针对操作系统以下的基础架构进行防御。

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

02 威胁模型

现状以及攻防双方的视角

安全不是什么...

- *不是堆切安全硬件设备
- *不是一个产品或者服务...(by Bruce Scheiner)
- *不是一个产品，而是一个持续不断的过程...(by Bruce Scheiner)
- *(安全审计)不是"扫描一堆端口"
- *不是业务部门的对立面

安全是什么...

- *是考虑"你能在不影响业务的情况下组织不被入侵吗？"
- *是最薄弱的防线将成为你的短板
- *是企业资源(机器和人)的风险管理
- *是考虑"有人能社工进入公司并且访问计算机，磁盘和磁带..."
- *是24 * 7 * 365...持续不断..并且永不停止
- *是以计算机科学为基础，关乎过程，方法论，成本，策略和人的复杂系统综合博弈

“我”眼中的完美方案

- *零信任
- *威胁情报
- *抗DDoS
- *云原生
- * KMS/HSM
- * ...

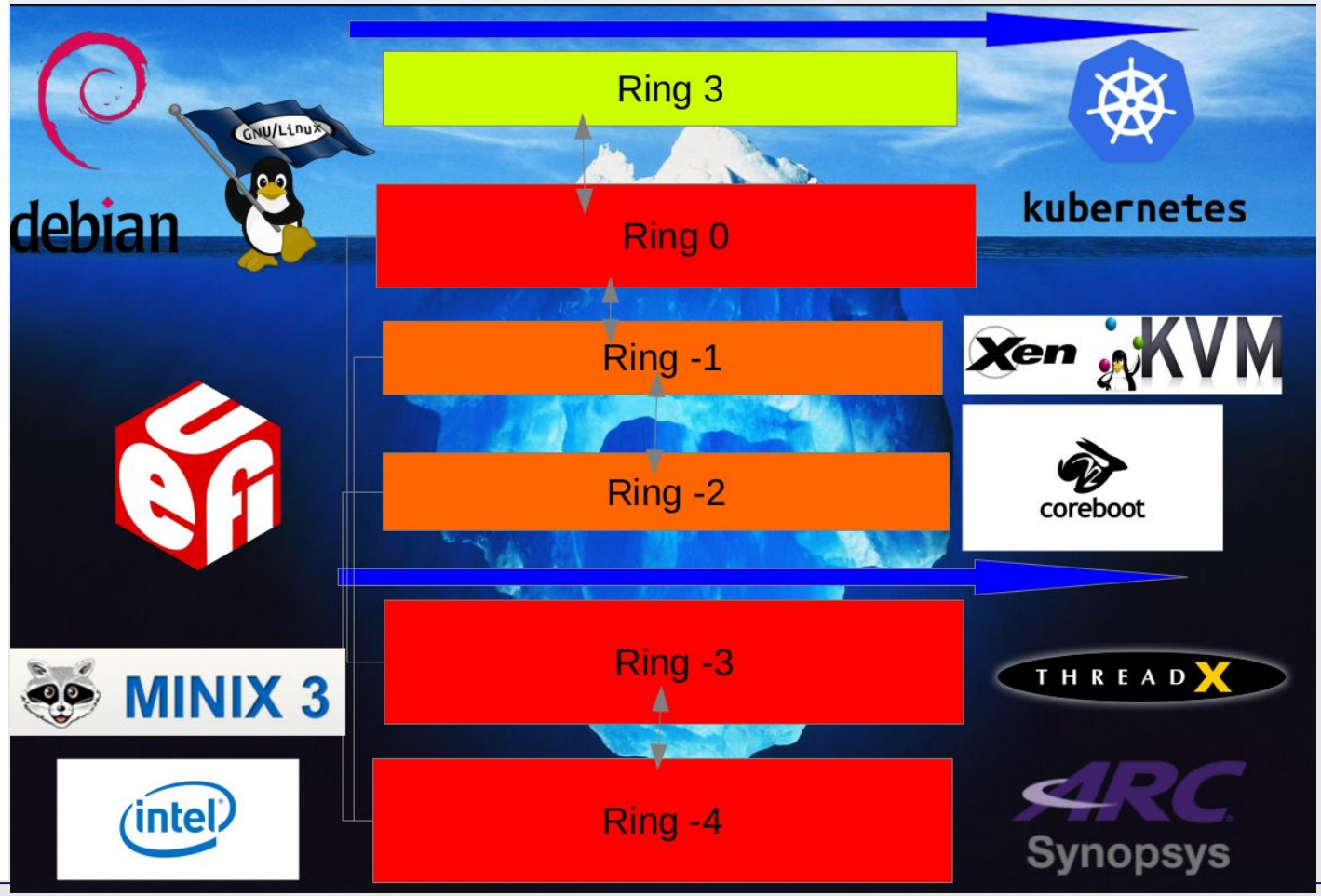
风险“完美”预期

企业生产环境实际风险

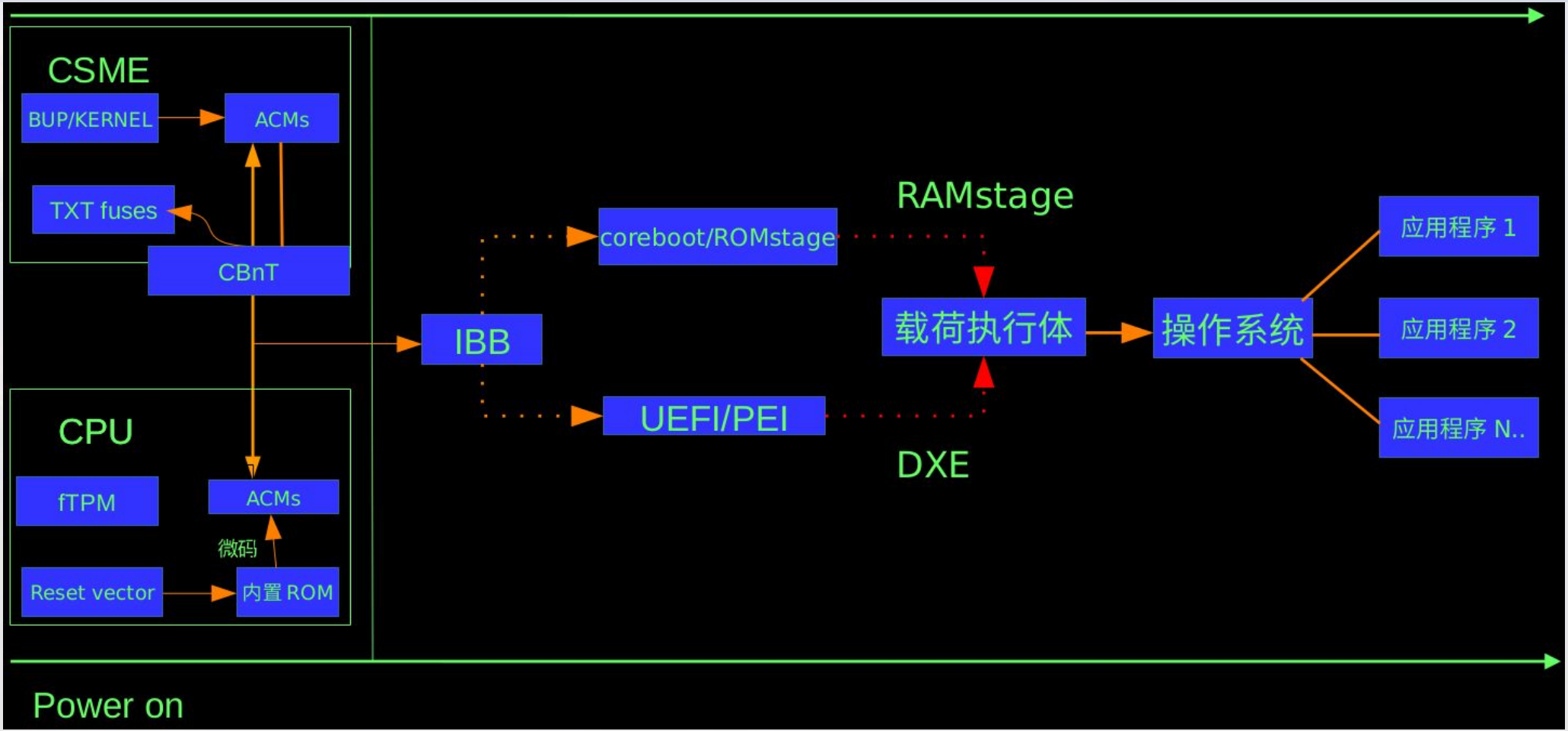

企业安全产品
Threat Intelligence
Data protection
SIEM
WAF
IAM
IDS/IPS
DoS protection
Operational Security
Secure software development
Encryption storage
DAC/MAC/RBAC
常规APT攻击
RING0 exploit detection
Kernel mitigation
TPM/TXT/DRTM
CnBT
Hardware Fault injection defense
SPI flash write protection
SMM rootkit detection
ME manufacturing mode
定向APT玩家
VISA/IOSF
ucode
PCB analysis
PCB golden image
RTL audit
Reproducible semiconductor fabrication process
Metadata protection
???
隐藏玩家

攻击“核心”？问题是哪里才是“核心”？

Ring 3	应用层
Ring 0	Linux 内核
Ring -1	虚拟化
Ring -2	SMM
Ring -3	CSME
Ring -4	指令集
	微码引擎
	集成电路 /PCB
	逻辑门
	晶体管
	物理学现象

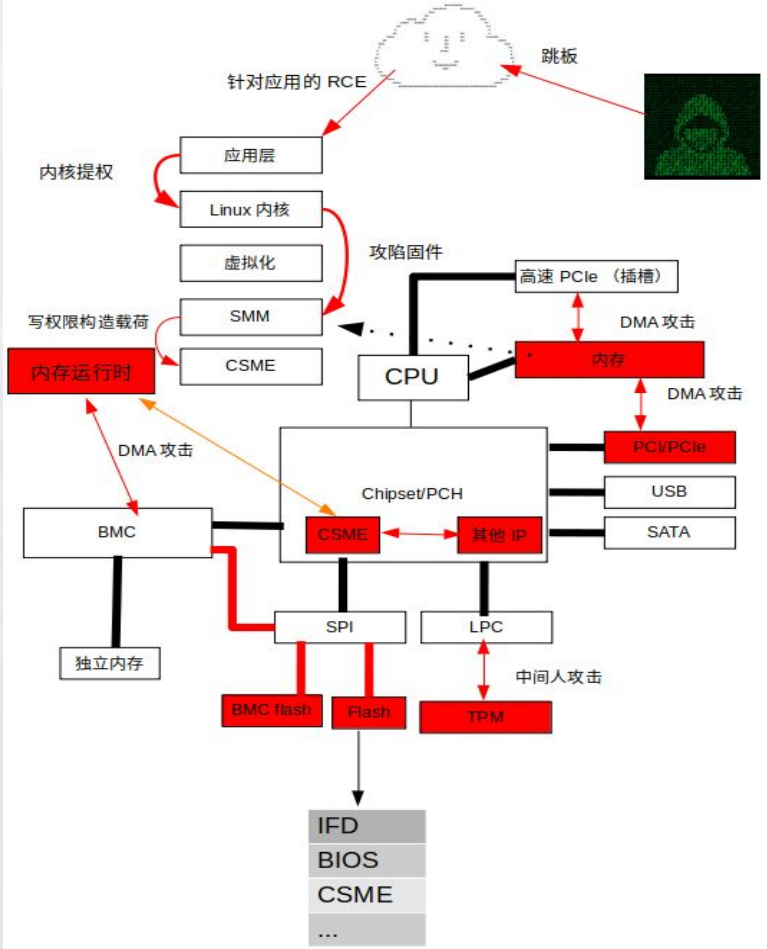


审视通用计算设备的启动过程:x86例子



高级威胁防护背景下的威胁模型之一

攻击路径:
* Ring 3 的漏洞利用(webshell或者应用程序的远程利用)获得普通执行权限
* 利用 Ring 0内核漏洞进行提权,这里值得注意的是虽然操作系统内核早已经不是 2007年“Attacking the CORE”上下文的那个”CORE“但依旧非常重要,因为内核是通向更底层的入口
* 从目前攻击样本来看不需要过多关注Ring -1虚拟化层。
* 通过绕过芯片组防护机制或者物理攻击攻陷Ring -2的固件,比如SMM,以达到获得写 SPI flash的能力。
* 触发 Ring -3(CSME)早期启动阶段(RBE,kernel 等在>=CSMEv11 版本中无法关闭的模块)或者 CSME 代码模块的 0day 或者已知漏洞(比如 SA-00086)以获得 CSME 完整控制权,攻击者可以使用 CSME 作为跳板开启 VISA 访问 PCH 的内部接口。



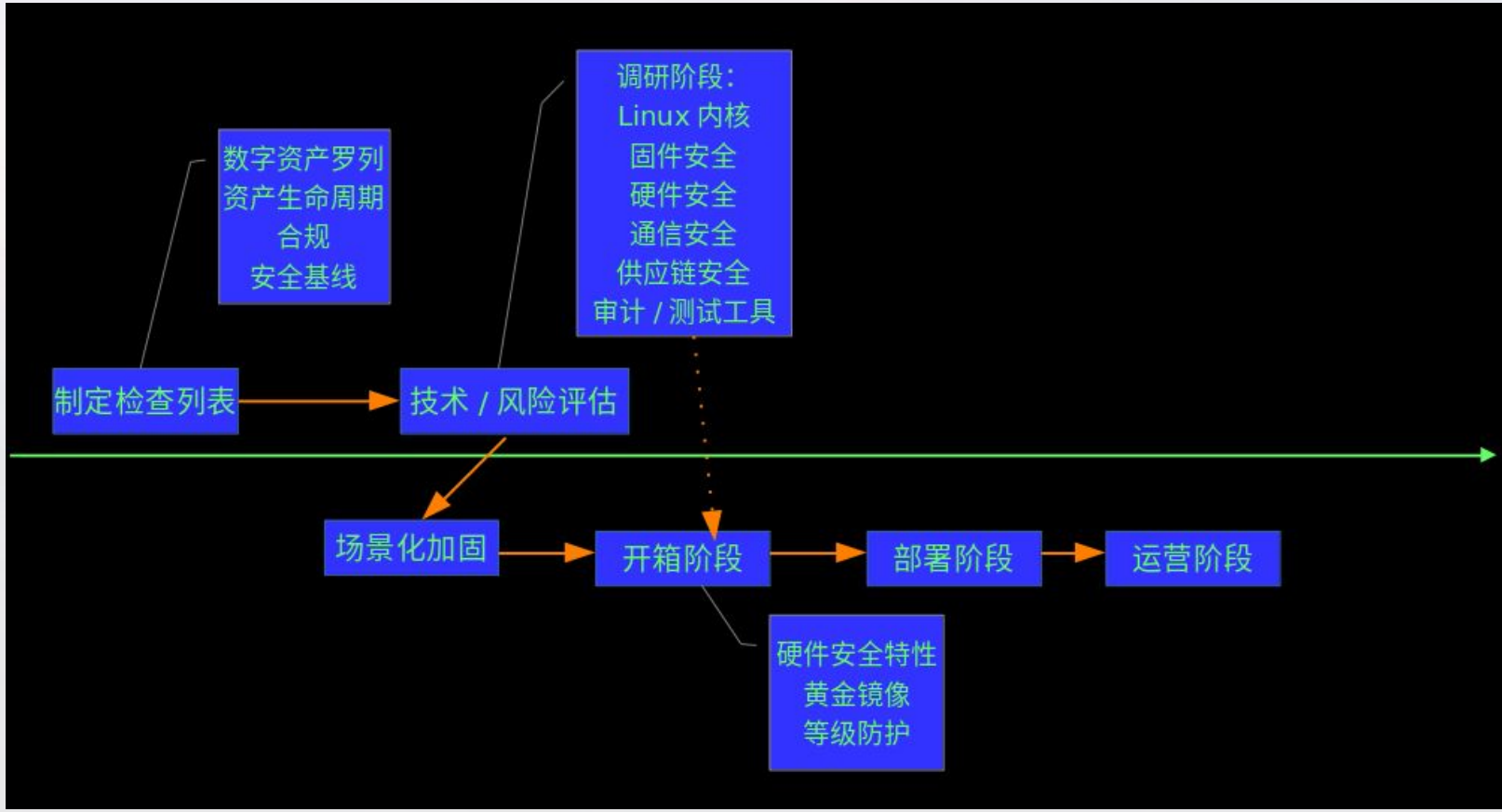
03 开源体系基础架构安全

打造赛博堡垒

主线和支线任务:对抗复杂性

主线任务:
* Ring 0:Linux内核
* Ring -1:虚拟化
* Ring -2:BIOS固件
* Ring -3:带外实现

支线任务:
*模糊测试(Fuzzing test)
* 供应链安全



Ring 0：Linux内核安全现状

* 过长的修复链条

* Bug修复不及时，发行版难以及时发现并且完成backport

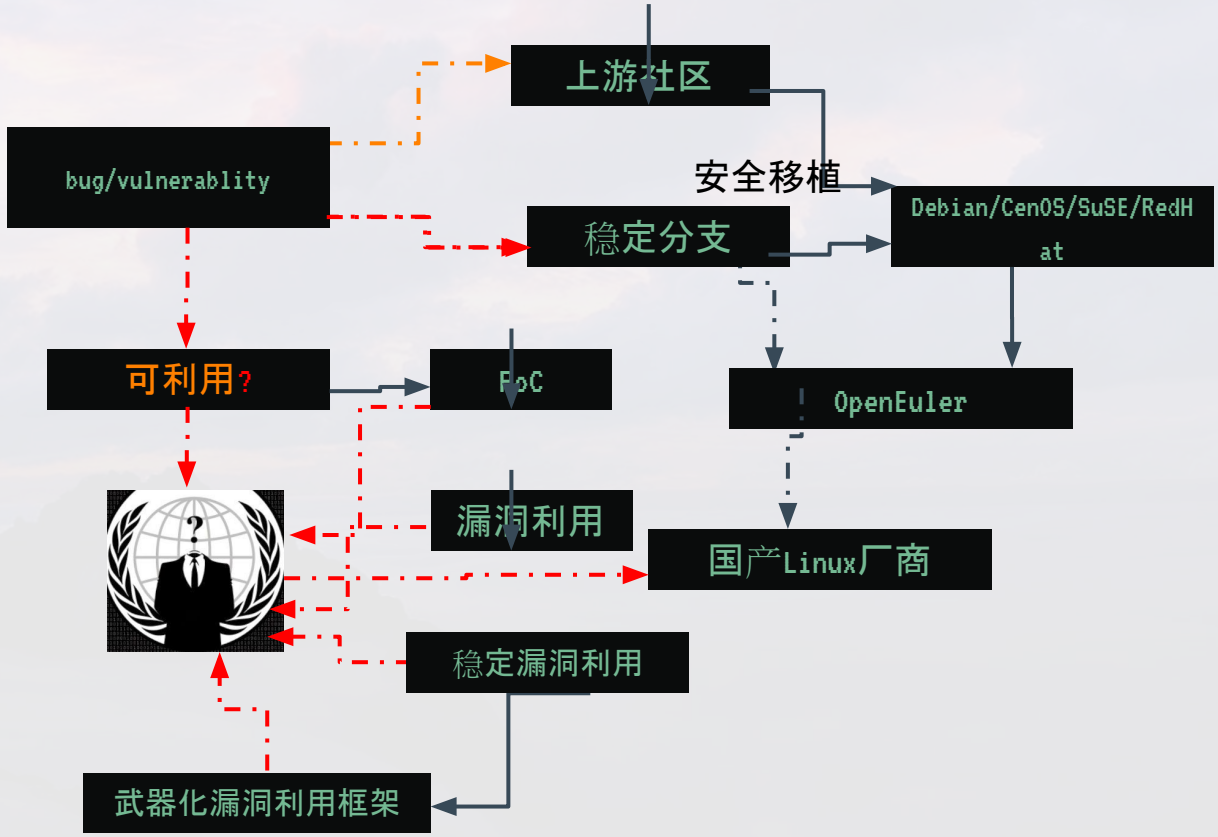
* Linux上游社区的”混淆即安全“哲学对于企业的风险

* 攻击者链条并不在乎Linux社区是否有CVE

* 2021年公开有CVE编号的漏洞为136个

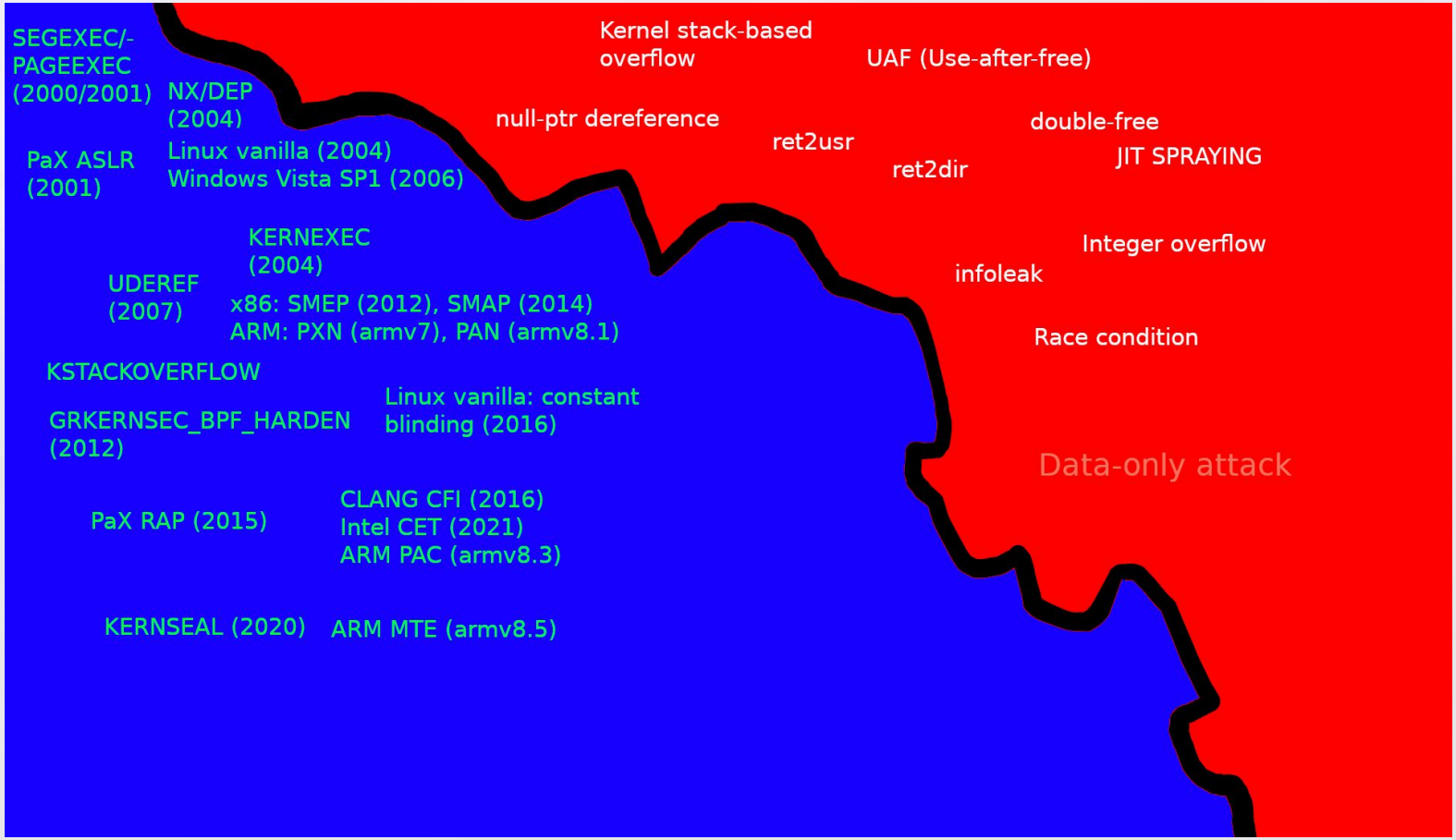
* 可利用的漏洞但并未有编号的,可能会在CVE的基础上上升50%甚至100%以上,攻击者定向打击利器。

* 有公开poc和exp的漏洞,会导致大规模入侵事件



Ring 0的长期对抗

* “疫苗”式防护率：
10%--99.3%
* 性能开销
1%--70%
* 价格因素
20美金—5000美金
/节点/年

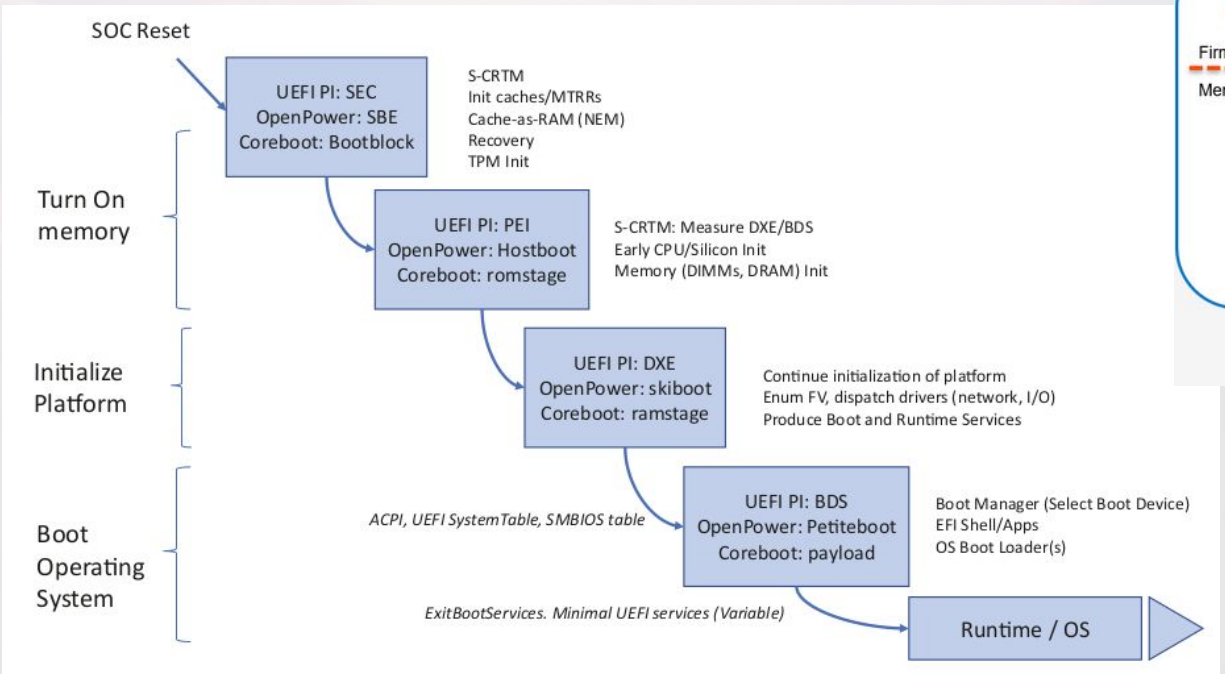


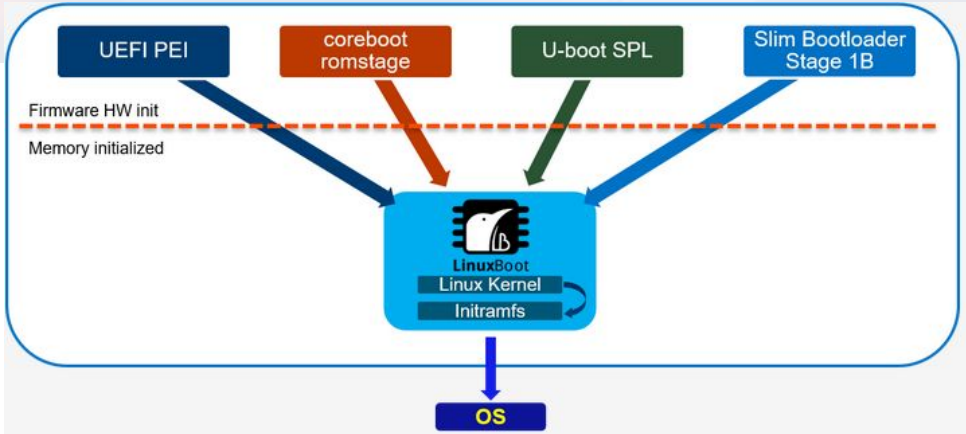
Ring -1：沉寂的样本

* 共享内核的防护机制
* 用户空间QEMU：
** 基线：减小攻击面
** seccomp沙箱
* 漏洞利用防护相对容易
* 未见大规模持久化样本

Ring -2:固件很复杂


Coreboot boot block
Coreboot ROM stage
Coreboot RAM stage, SMM Load
Payload
Final OS


SOC Reset
UEFI PI: SEC
OpenPower: SBE
Coreboot: Bootblock
S-CRTM
Init caches/MTRRs
Cache-as-RAM (NEM)
Recovery
TPM Init
Turn On memory
UEFI PI: PEI
OpenPower: Hostboot
Coreboot: romstage
S-CRTM: Measure DXE/BDS
Early CPU/Silicon Init
Memory (DIMMs, DRAM) Init
Initialize Platform
UEFI PI: DXE
OpenPower: skiboot
Coreboot: ramstage
Continue initialization of platform
Enum FV, dispatch drivers (network, I/O)
Produce Boot and Runtime Services
ACPI, UEFI SystemTable, SMBIOS table
UEFI PI: BDS
OpenPower: Petiteboot
Coreboot: payload
Boot Manager (Select Boot Device)
EFI Shell/Apps
OS Boot Loader(s)
Boot Operating System
ExitBootServices. Minimal UEFI services (Variable)
Runtime / OS


UEFI PEI
coreboot romstage
U-boot SPL
Slim Bootloader Stage 1B
Firmware HW init
Memory initialized
LinuxBoot
Linux Kernel
Initramfs
OS

Ring -2:门槛和复杂性

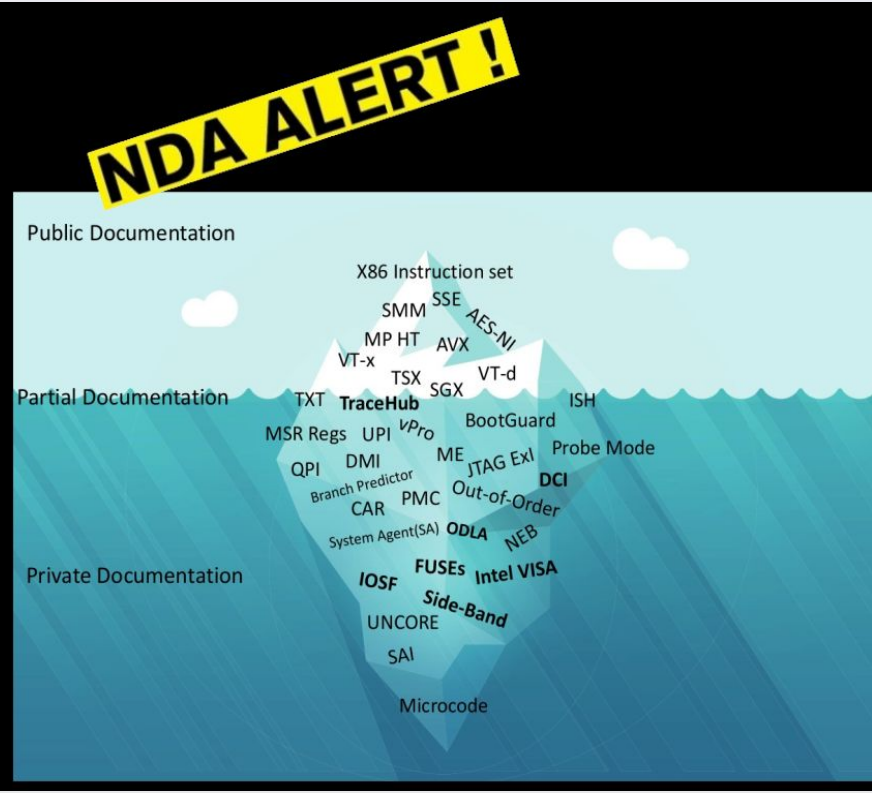
DAL

Debugger

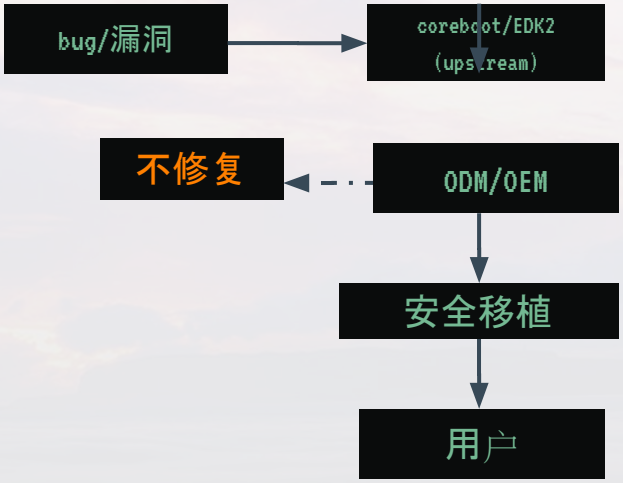
TXT/PFR

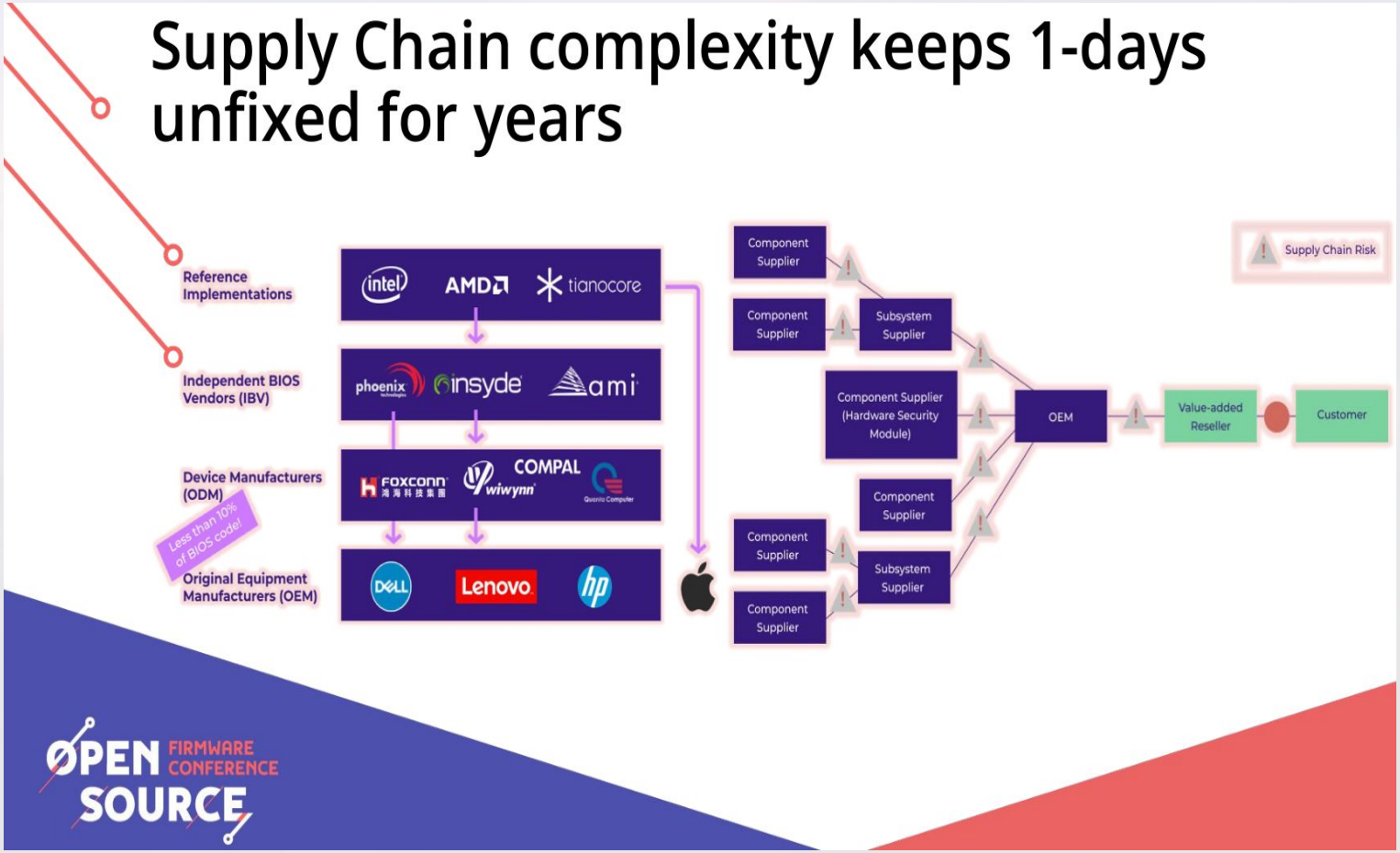
FSP

Microcode



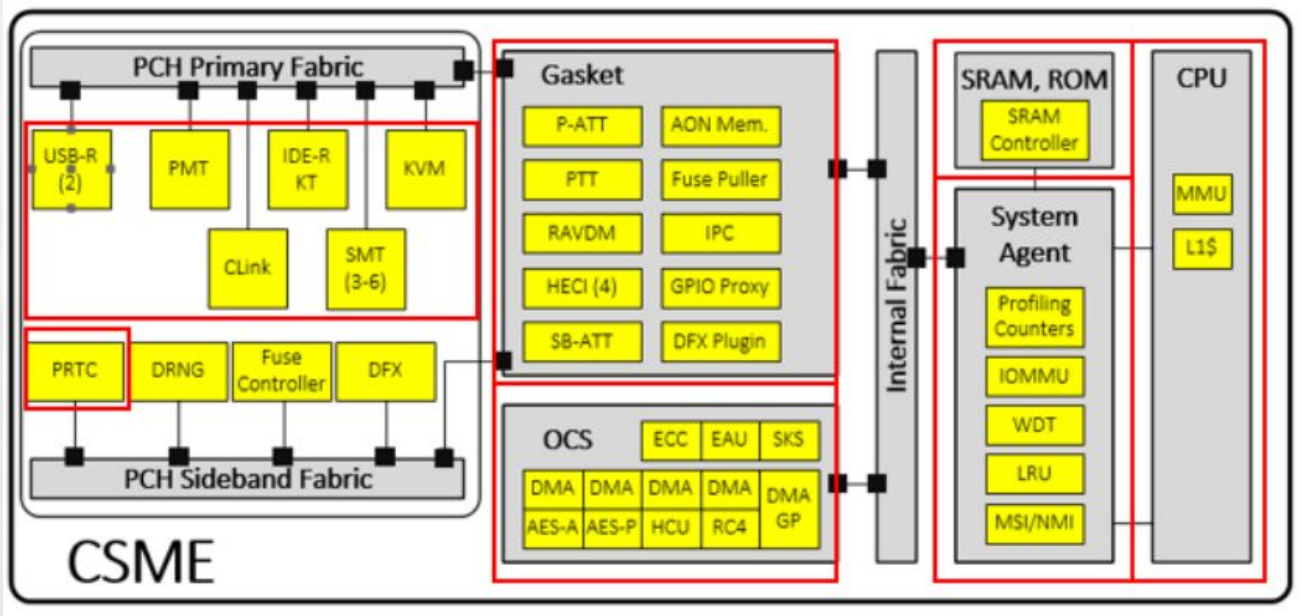
Ring -2：固件修复和供应链也很复杂





Ring -3：图灵机中的图灵机

*存在于2006年后的每台x86设备中
*独立系统，PCH中最重要IP
*多个实现，桌面/服务器/嵌入式



Ring -3：图灵机中的图灵机

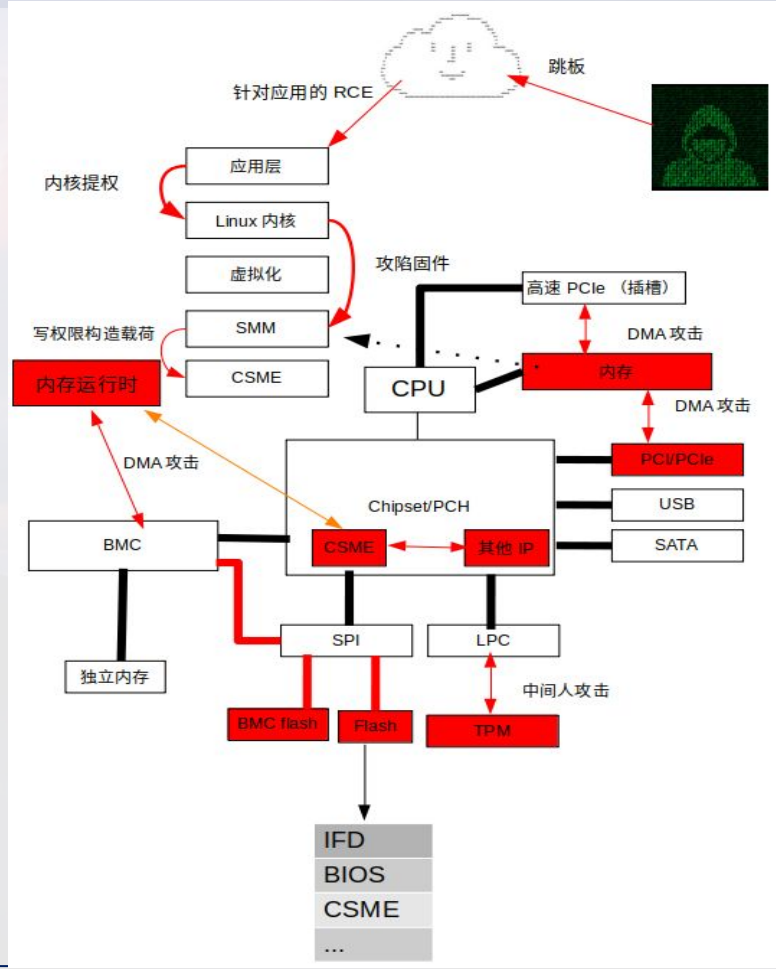
	ME	ME	ME	ME	ME
版本	1.x – 5.x	6.x – 10.x	11.x	12.x	15.x
硬件核心	ARCTangent -A4	ARCompact	Quark	Quark	Quark(?)
指令集	ARC (32-bit)	ARCompact(32/16)	x86(32-bit)	(32-bit) x86	x86 (32-bit)
防御特性	N/A	N/A	NX	SMEP	CET/CFI
操作系统	??	ThreadX	MINIX	MINIX	MINIX
对应SPS版本	SPSv1.x	SPSv2.x – v3.x	SPSv4.x	SPSv5.x	SPSv6.x

Ring -3:猎杀暗影 --> 透明度提升

Intel CSME	Before	After
Neutralization	Boot every 30 mins	Minimizing it by unsigned code removal
Kill switch	N/A	Found HAP/Altmedisable bit
Internal fabric	No access without NDA	More knowledge of PCH/IOSF/VISA
CSME security	RTOS without basic mitigation	Modern mitigation and bug hunting process
Official material	No public release	Intel released security white paper for CSME v14/v15

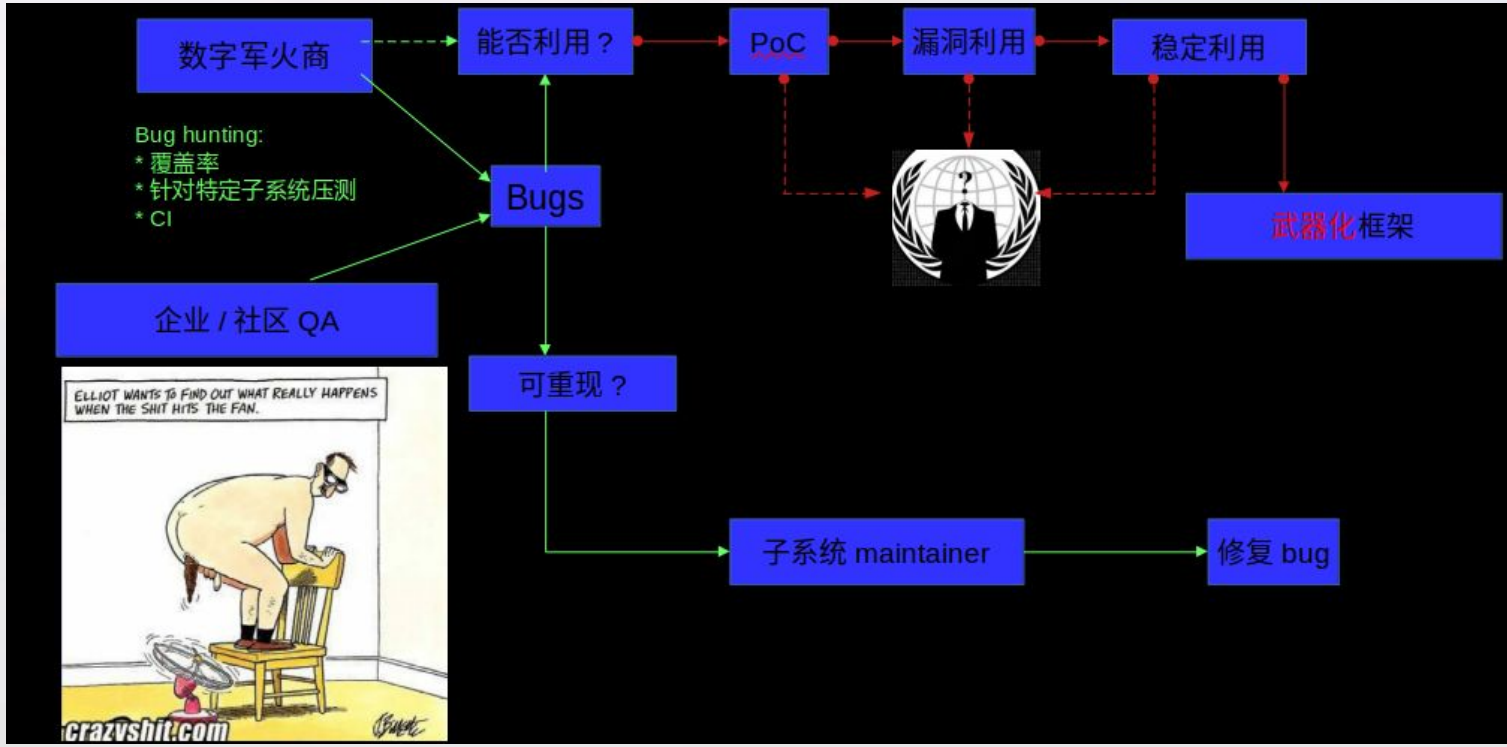
威胁模型

* Linux内核依然是地下世界的入口
*独立银弹方案无法存活，比如SGX
*可信计算的核心：
** Verified Boot
** Measured Boot
* 安全开箱的重要性



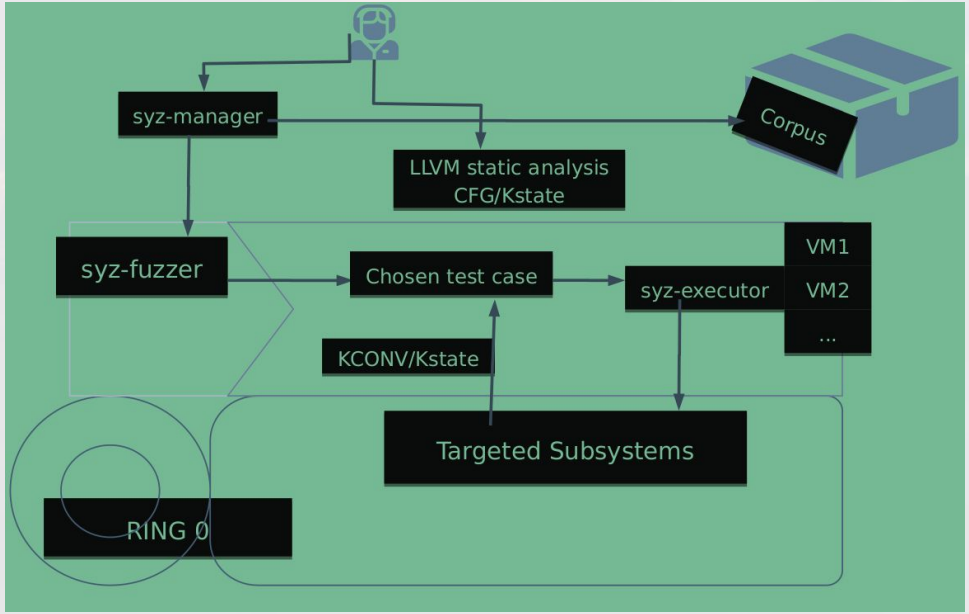
支线任务之状态导向的Linux内核模糊测试

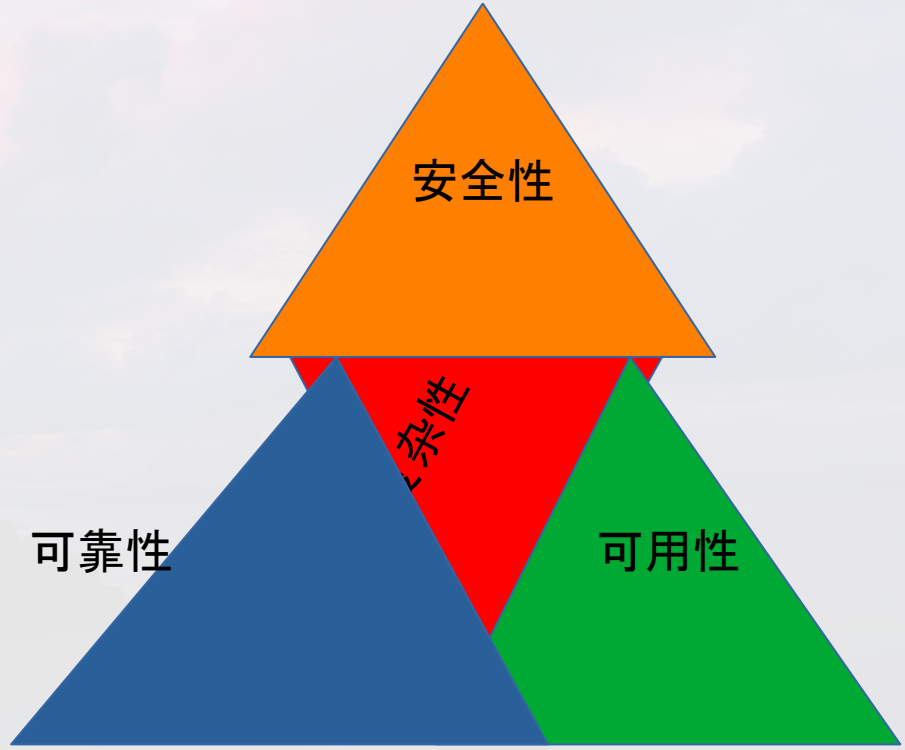
* Fuzzing的视角
**安全导向，漏洞挖掘
** QA导向，覆盖率压测
*有限算力组合方案，比如：
** 硬件20 core + 20GB
** 特定子系统>=70%覆盖率
** 用时小于20小时



支线任务之状态导向的Linux内核模糊测试

*为什么针对Linux内核的QA/fuzzing对防护重要？
*对业务稳定性同等重要
* 驯服复杂性的关键环节





支线任务之供应链风险

“We know it's possible both because the NSA has apparently done it, but also because I'VE done it." at Chaos Communication Congress
*不论报道是否真实，威胁真实存在

Supermicro audit finds no evidence of back doors

Written by
Gareth Halfacree

December 12, 2018 | 10:39

Tags: #charles-liang #david-weigand #hardware-back-door #insecurity #motherboards #raju-penumatcha #security #server #supermicro #supply-chain

Companies: #amazon #apple #bloomberg #super-micro-computer

Bloomberg

The Long Hack: How China Exploited a U.S. Tech Supplier

For years, U.S. investigators found tampering in products made by Super Micro Computer Inc. The company says it was never told. Neither was the public.

By Jordan Robertson and Michael Riley
February 12, 2021, 5:00 AM

In 2010, the U.S. Department of Defense found thousands of its computer servers sending military network data to China—the result of code hidden in chips that handled the machines' startup process.

The Big Hack: How China Used a Tiny Chip to Infiltrate U.S. Companies

The attack by Chinese spies reached almost 30 U.S. companies, including Amazon and Apple, by compromising America's technology supply chain, according to extensive interviews with government and corporate sources.

Apple deleted server supplier after finding infected firmware in servers [Updated]

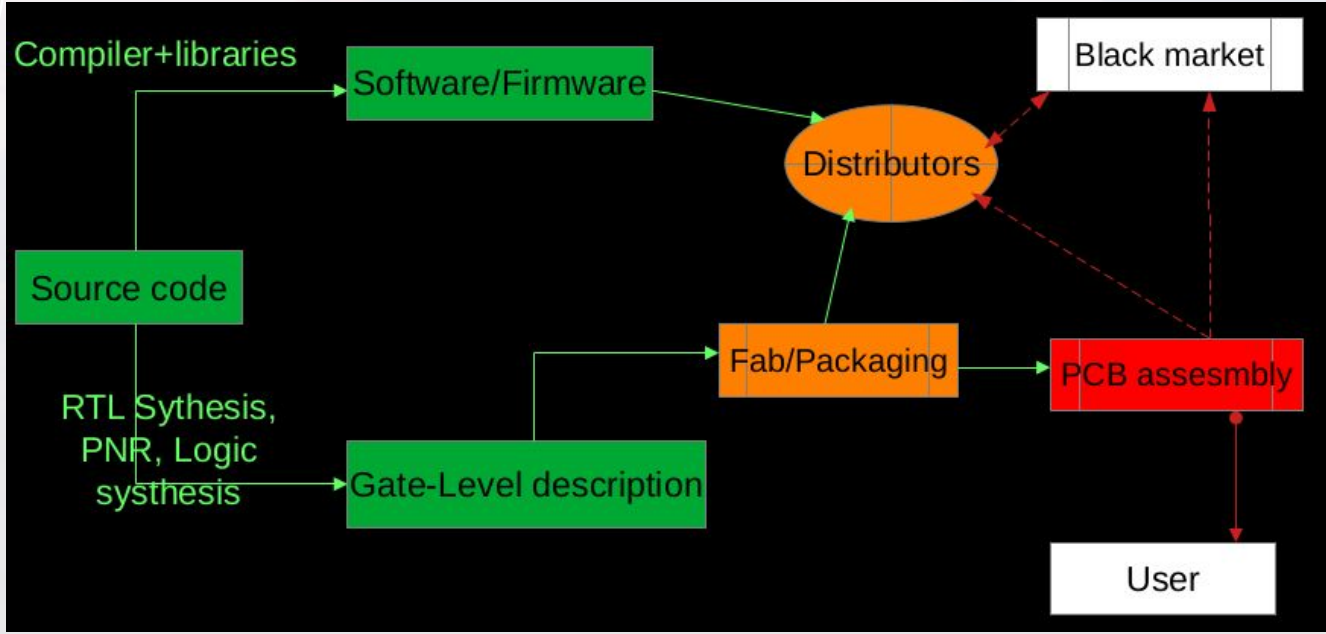
Report: Siri, internal development servers affected by fake firmware patch.

SEAN GALLAGHER - 2/24/2017, 4:49 PM

硬件供应链复杂性

* 例子Cheap PCB
**基于stm32*
**成本10美金以内

device	package	quantity
Capacitor 10uF	0603	2
Capacitor 10nF	0603	1
Capacitor 100nF	0603	8
Capacitor 22pF	0603	2
Schottky diodes 1N5817WS	SOD-323	1
light-emitting diode Red	0603	1
light-emitting diode Blue	0603	1
light-emitting diode Yellow	0603	1
Fuse 500mA	0805	1
Fuse 100mA	0805	1
USB C Receptacle	Palconn UTC16-G	1
2×4 2.54mm PinHeader		1
1×25 2.54mm PinHeader		2
Transistor S9012	SOT-23	2
Resistor 1K	0603	1
Resistor 10K	0603	6
Resistor 5.1K	0603	3
Resistor 22	0603	2
Resistor 1K5	0603	2
Button KMR241G		1
AMS1117-3.3	SOT-89	1
STM32F103C8T6	LQFP-48	1
Crystal 8MHz	SMD_3225	1



04 结论

没有银弹

有完美防御方案吗？没有银弹！

谢谢大家！

- * Q/A和交流！
- *关注我司社交媒体
- *谢谢
- * 邮箱：shawn.chang@hardenedvault.net

https://www.zhihu.com/org/sai-bo-bao-lei-hardenedvault

参考引用

- * The Huawei and Snowden Questions
- https://link.springer.com/book/10.1007/978-3-319-74950-1
- * Intel Visa: Through the Rabbit Hole
- https://github.com/ptresearch/IntelVISA-BH2019/blob/master/asia-19-GORYACHY-REMOLOV-Intel-Visa-Through-the-Rabbit-Hole.pdf
- * The Long Hack: How China Exploited a U.S. Tech Supplier
- https://www.bloomberg.com/features/2021-supermicro/
- * Open Source is Insufficient to Solve Trust Problems in Hardware
- https://media.ccc.de/v/36c3-10690-open_source_is_insufficient_to_solve_trust_problems_in_hardware

参考引用

- * Try Harder 2 Be Yourself
- http://2012.zeronights.org/includes/docs/Keynote%20FX%20-%20Try%20harder%202%20be%20yourself.pdf
- * Linux kernel mitigation checklist:
- https://hardenedlinux.github.io/system-security/2016/12/13/kernel_mitigation_checklist.html
- * Ring 0: Linux kernel vulnerablity & exploitation & silent fixes
- https://github.com/hardenedlinux/grsecurity-101-tutorials/blob/master/kernel_vuln_exp.md
- * Intel ME info:
- https://github.com/hardenedlinux/firmware-anatomy/blob/master/hack_ME/me_info.md

参考引用

- * 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 stats
- https://github.com/hardenedlinux/hardenedlinux_profiles/tree/master/coreboot

谢谢大家

安天冬训营 wtc.antiy.cn