

Linux Kernel Validation Suite

—— 英特尔内核测试套件

孙毅 | Intel

Linux Kernel Validation Suite

Intel 内核测试套件

LKVS是什么



如何使用LKVS



测试范围



典型案例



LKVS 发展时间线



LKVS 是什么

一个轻量级、低耦合、高覆盖的内核测试框架

600+

共计测试用例

20+

覆盖硬件/内核属性

3

合作内核社区

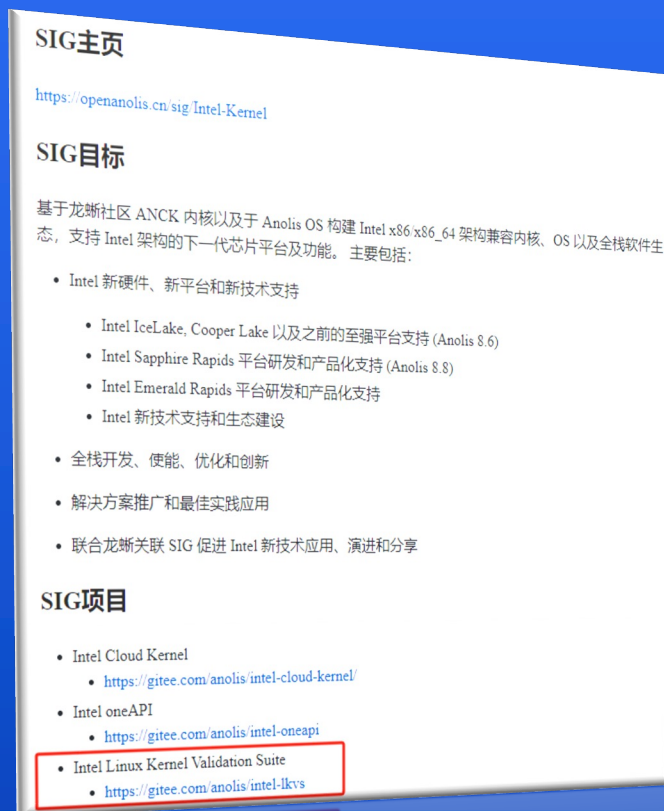


LKVS 测试数量趋势



LKVS 如何使用

<https://github.com/intel/lkvs>



<https://gitee.com/openeuler/intel-lkvs>

编译

- 编译完整项目
make
- 编译单个属性测试
cd <folder>; make

运行

- 运行测试集合
./runtests -f <cmdfile> -o <logfile>
- 运行单个测试用例
参考单个属性目录中的**README**文件

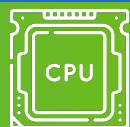


LKVS 测试覆盖范围

测试范围



CPU



XSAVE / XState

FRED

CPU topology

SDSI (Software Defined Silicon)

Thermal

UMIP (user-mode Instruction Prevention)

PMU (Performance Mon)

PT (Performance Trace)

Xsave workload

In-field scan

Split Lock detection

Power



Intel_idle

PState

SST (Speed Select Technology)

TPMI_UFS(Uncore Frequency Scaling)

RAPL (Running Average Power Limiting)

Security



TDX (Trust Domain Extensions)

CET (Control Flow Enforcement Technology)

LKVS中的明星测试 - TDX

Intel® Trust Domain Extensions (Intel® TDX)



Intel® Trust Domain Extensions (Intel® TDX)

可信计算技术

基于硬件隔离的虚拟机，防止敏感数据和应用被未授权的访问



TDX compliance(TDX 一致性测试)

在TDVM中，内核测试模块，通过特权指令读写数据，例如：CUID, MSR, CR 等



TD实例中的 MCE 问题

在pre-release 测试中，发现并定位了 TD实例中的 MCE 问题



LKVS中的明星测试 - CET

Control-flow Enforcement Technology (CET)



Control-flow Enforcement Technology (CET)

控制流增强技术，包含了两个组件：shadow stack 和 Indirect branch tracking



Shadow Stack

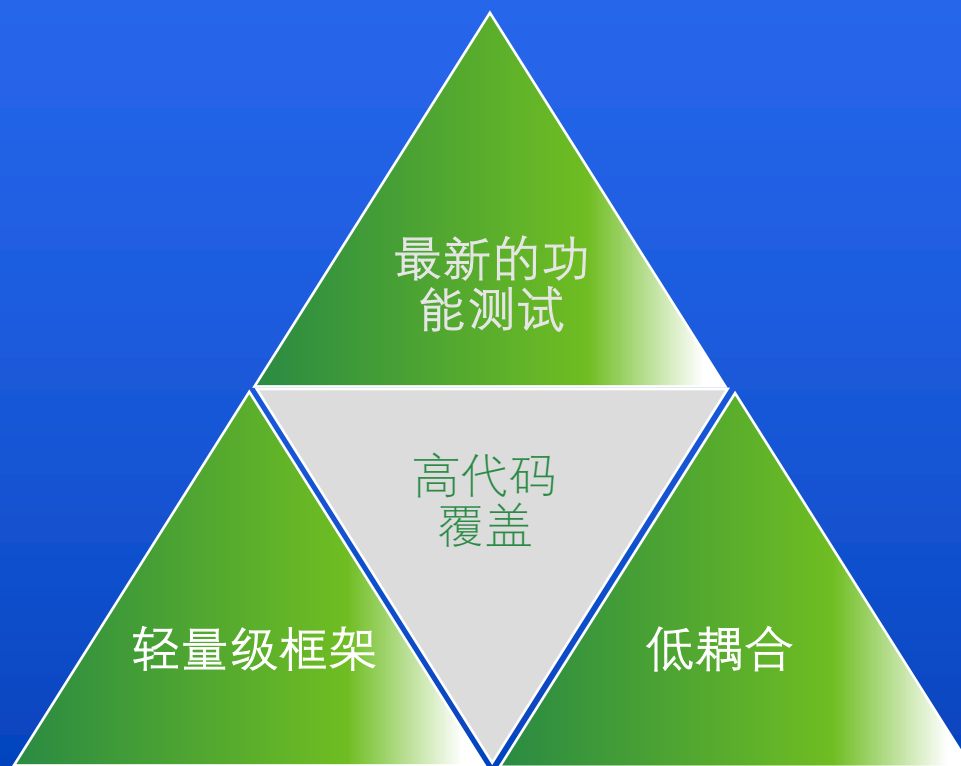
防止ROP(Return-Oriented Programming) 攻击，
通过hack return 指令对系统进行的攻击



IBT(Indirect Branch Tracking)

防止JOP(Jump-Oriented Programming)攻击，
通过hack借助寄存器跳转，进行的攻击

LKVS 优势



联系我们

Intel Core Linux Validation



- Email: yi.sun@intel.com
- Gitee: <https://gitee.com/openeuler/intel-lkvs/issues>



THANKS



