基于硬件可信执行环境技术的隐私计算

王文浩

中国科学院信息工程研究所

广西 • 桂林

机密计算(Confidential Computing)

Microsoft

intel SGX Tool

Asylo: An open and flexible framework for enclave applications

Baidu

MesaTEE

什么是机密计算

机密计算(Confidential Computing)关注于保护使用中的数据的安全性。

- 作为对比，传统加密技术等主要保护数据传输和存储中的安全性。
- 与同态加密、多方安全计算、可搜索加密、零知识证明等不同，机密计算的底层技术是可信执行环境(TEE)技术。
- 应用场景可包括云端(服务器)、移动端、边缘设备等。

什么是可信执行环境(TEE)

1. **执行环境**：描述了一组该环境与外界的软、硬件接口，例如指令集、隔离要求等
2. **可信执行环境**：目标是确保一个任务按照预期执行
   ① 初始状态的机密性、完整性
   ② 运行时状态的机密性、完整性
3. 分类
   ① 软件可信执行环境
   - Overshadow[CGL+,ASPLOS'08]，SP³[YS,VEE'08]，CloudVisor[ZCC+,SOSP'11]，InkTag[HKD+,ASPLOS'13]，Virtual Ghost[CDA,ASPLOS'14]，HypSec[LKN,Security'19]等

   ② 硬件可信执行环境

根据场景需要，TEE的设计和实现不同

移动端的TEE

假如可以按照我的要求定制一台手机：

- 需要指纹支付功能，需要保护支付、指纹等数据
- 我可能会安装不信任的app
- 手机系统可能存在安全漏洞
- 可能会root/越狱

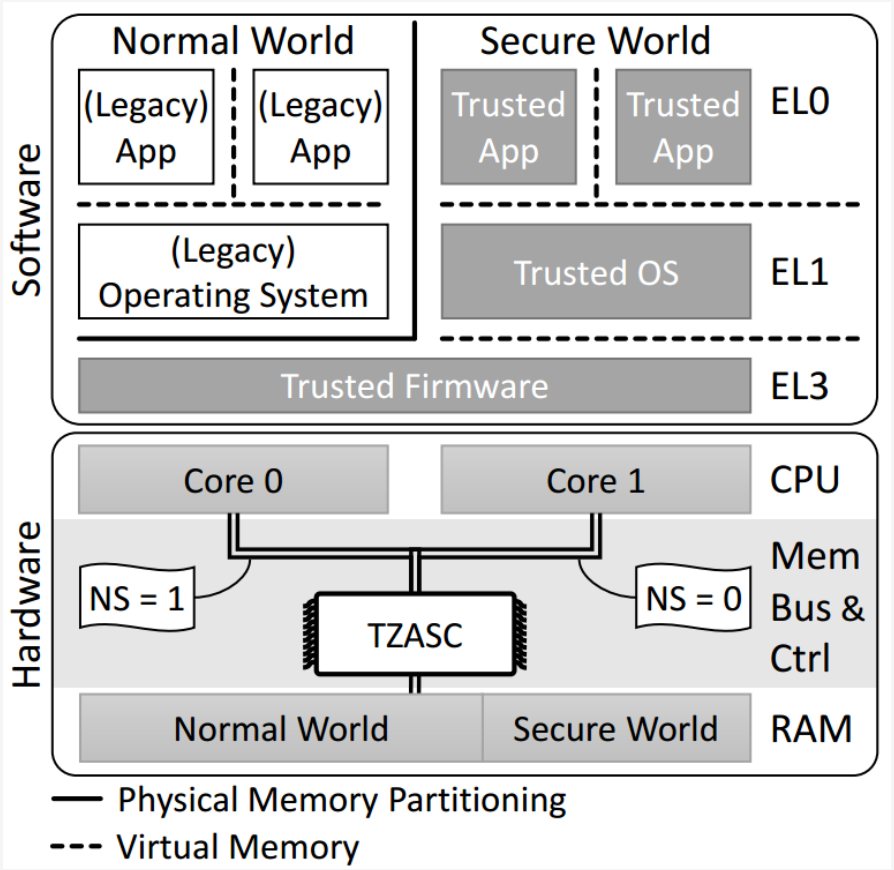
指纹数据及其使用在TEE中进行处理

- TEE与一般app隔离，仅保存调用接口
- 即使是手机系统被攻破，TEE中数据仍能得到保护

移动端的TEE

以ARM TrustZone for Cortex-A为例

- 安全世界和非安全世界
- TEE：构建在硬件之上的软件运行环境
- 比较典型的信任应用(TA)
  - 移动支付、钱包、认证
  - 可信密钥存储、数字版权保护
- 可信计算基(TCB)
  - 硬件
  - 安全世界的所有软件代码

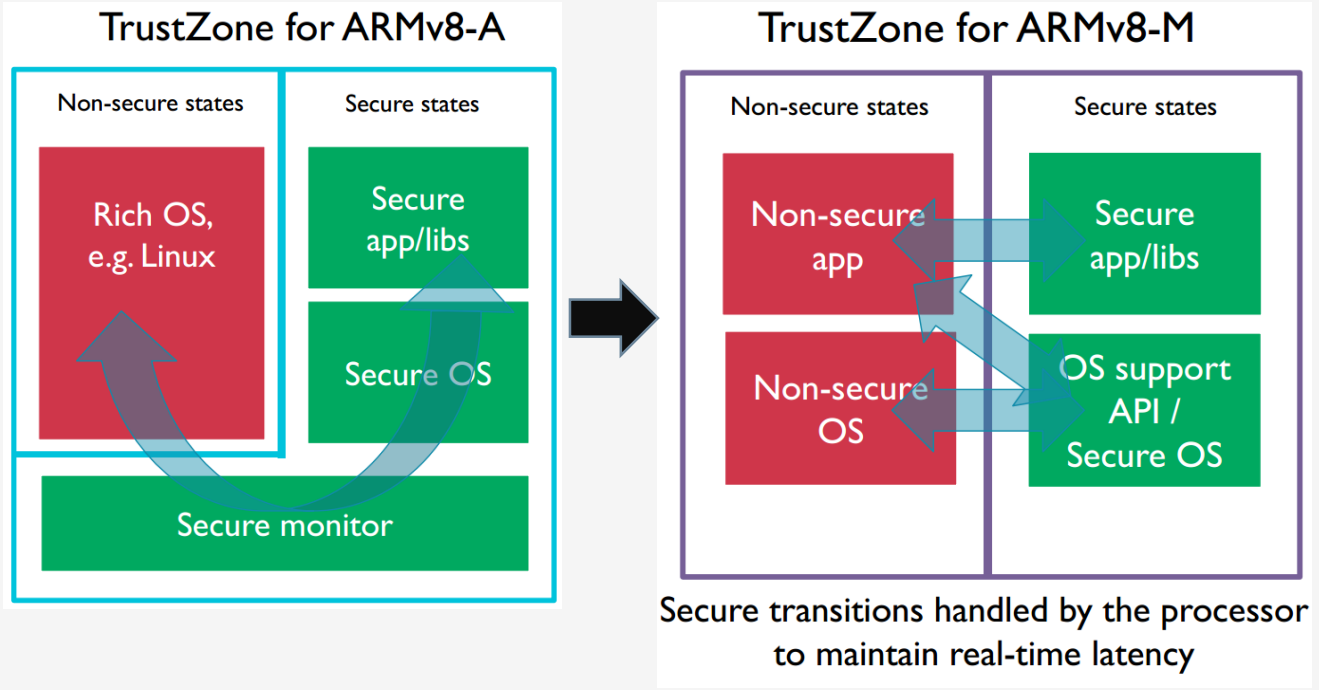


ARM TrustZone for Cortex-A

边缘端的TEE

以ARM TrustZone for Cortex-M为例

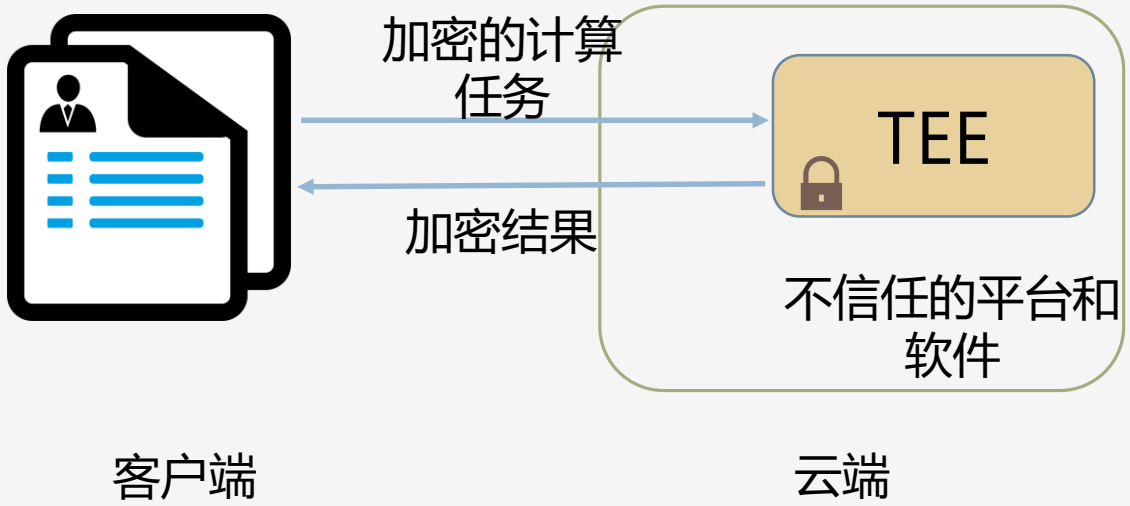
- 安全世界和非安全世界
- TEE：构建在硬件之上的软件运行环境
- 对TEE的要求
  - 低功耗
  - 实时处理
  - 快速切换
  - 低中断时延



云端的TEE

对TEE的要求：

- 远程认证
- 抗软件攻击
- 抗物理攻击
- 低权限



云端的TEE之AMD SEV

对TEE的要求：

- 远程认证

  使用平台背书密钥签名的证书链，向远程用户证明 ☑

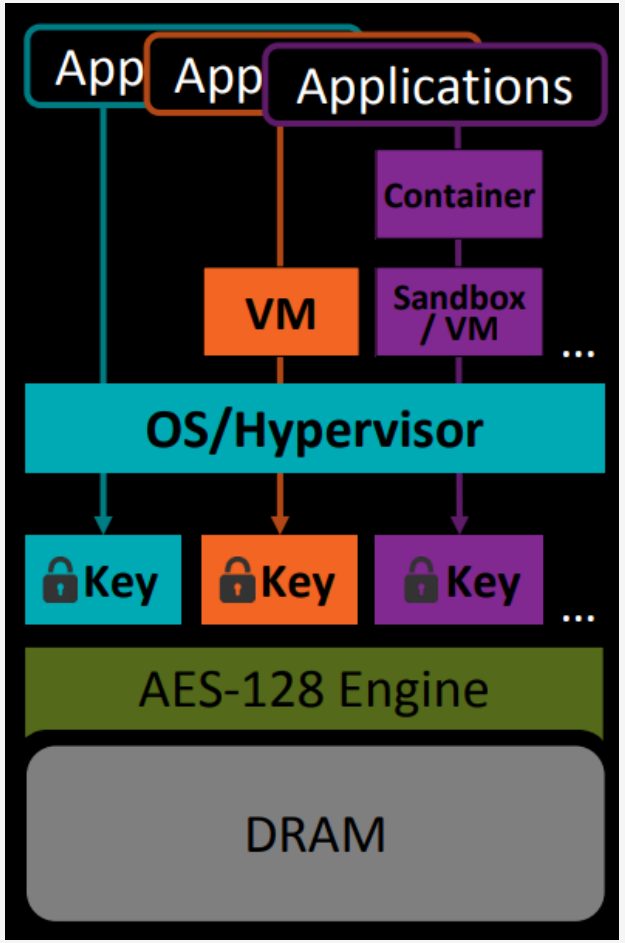
- 抗软件攻击 ☑

- 抗物理攻击

  每个VM的物理内存是加密的 ☑

- 低权限

  VM的资源调度仍然由Hypervisor管理 ☑



云端的TEE之AMD SEV

但是目前版本的AMD SEV仍不能用来支持机密（隐私）计算：

- 远程认证功能被发现严重漏洞[BWS,CCS'19]
  - 目前未完全修复
- VM Exit后，VM寄存器信息明文存储造成任意数据泄露[HB2017,SIGPLAN Notices 2017]
  - 目前未修复
- 物理内存加密缺乏完整性检查[MHH+,EUROSEC'18], [MHH19,CODASPY'19)]
  - 目前未修复
- 未保护的IO操作造成数据泄露[LZL+,Security'19)]
  - 目前未修复

云端的TEE之Intel SGX

Intel 公司的 TEE 的实现

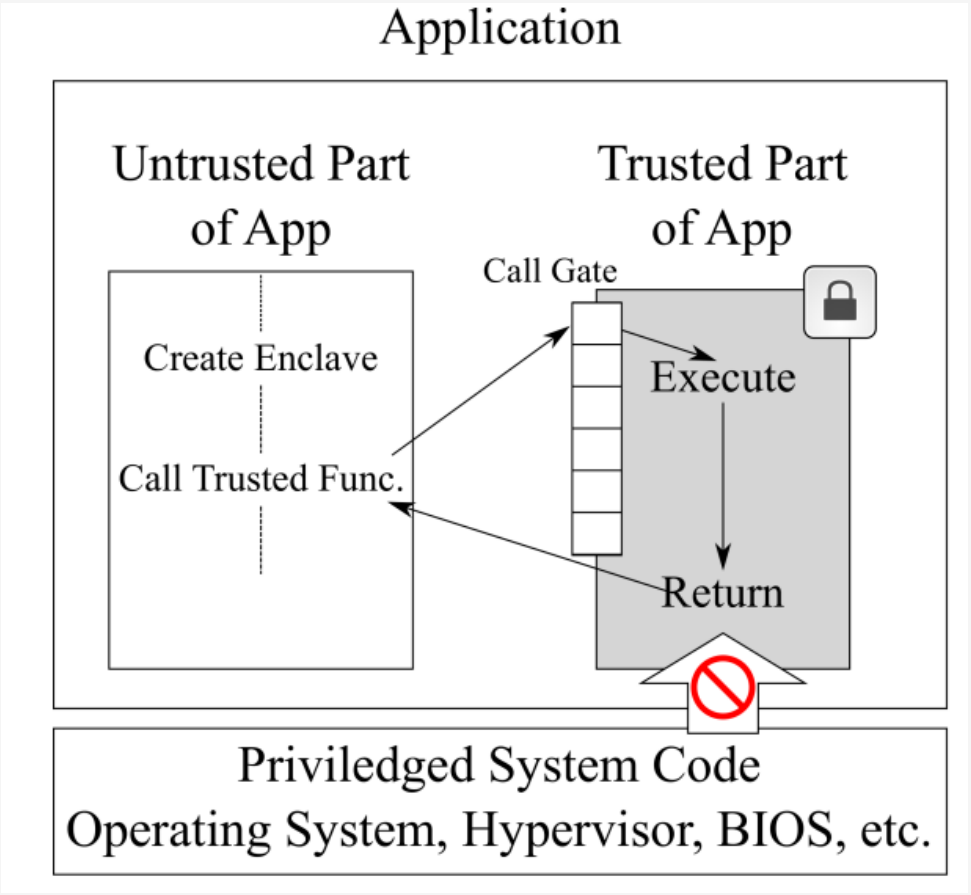
- 嵌入在进程中的TEE
- TCB仅包含CPU和TEE代码本身
- TEE代码运行在用户态(ring-3)

远程认证 ☑

抗软件攻击 ☑

抗物理攻击 ☑

低权限 ☑



云端的TEE之Intel SGX

远程认证

① Enclave创建及度量(软件身份)

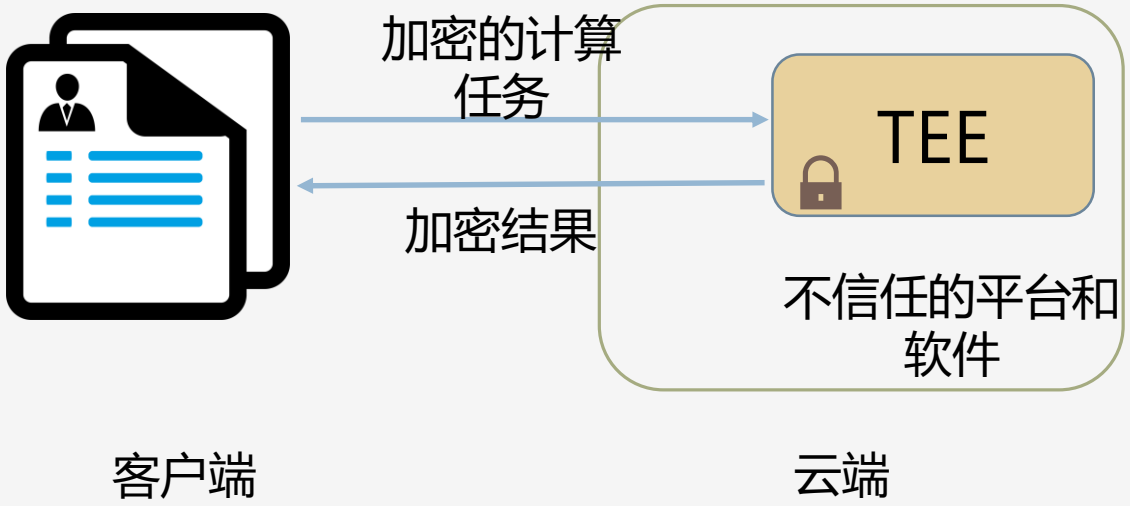
② 生成硬件签名的report

③ Report发送给远程用户

④ 远程用户将report转发至IAS，IAS验证report

⑤ 远程用户验证软件身份

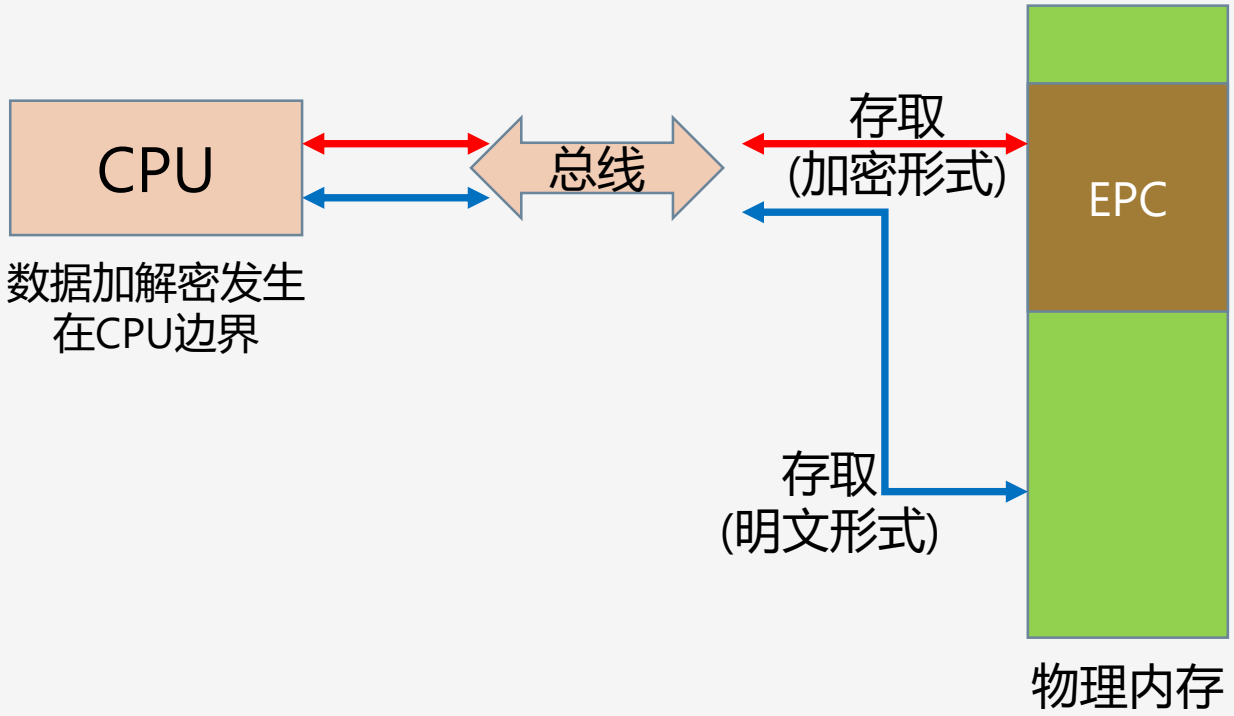
⑥ 在此过程中完成基于ECDH的密钥协商



云端的TEE之Intel SGX

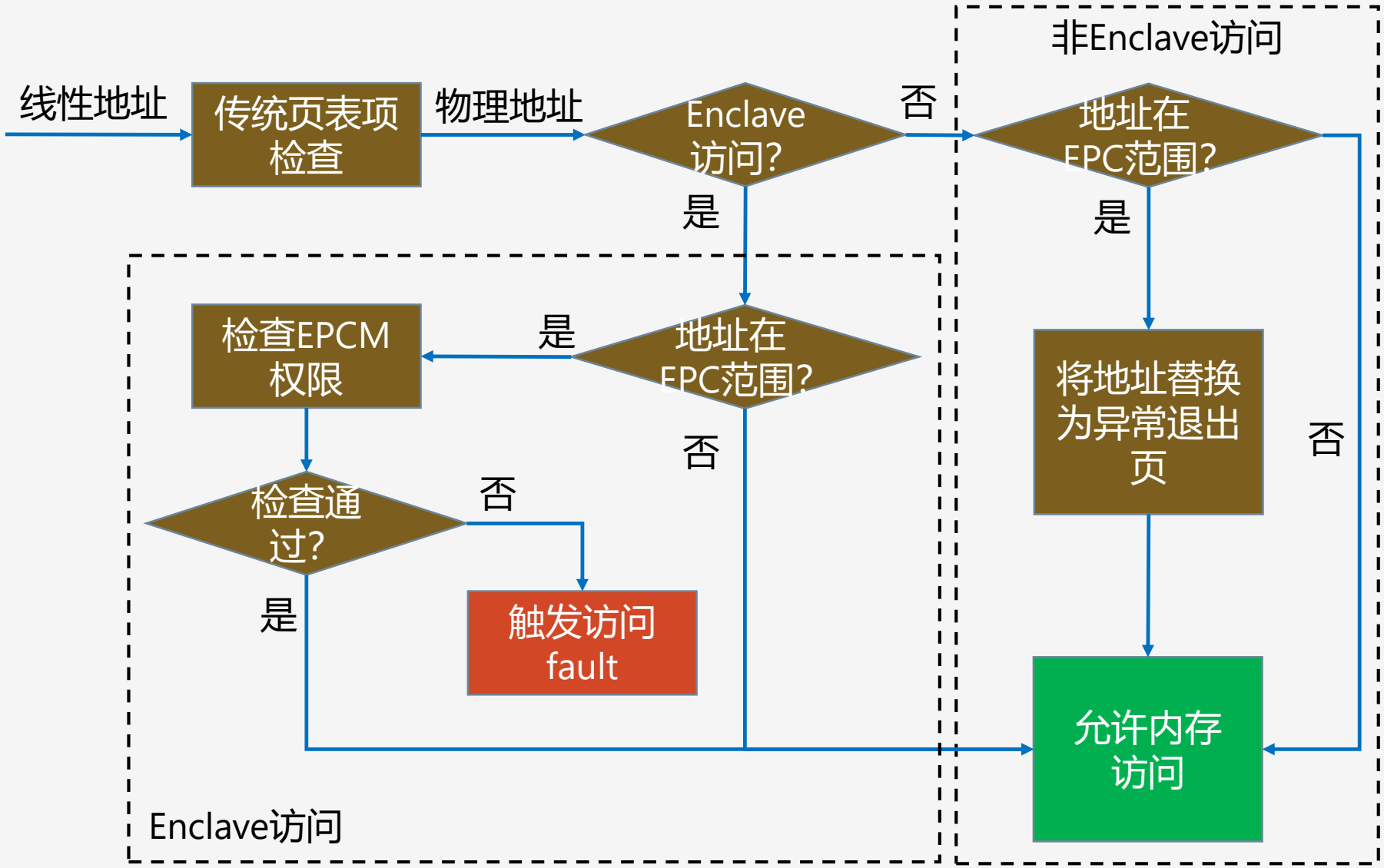
抗物理攻击

- 物理内存的加密区域
- 数据在总线、内存是加密的
  - 对抗bus snooping/cold boot等攻击
- 只有在CPU内才解密

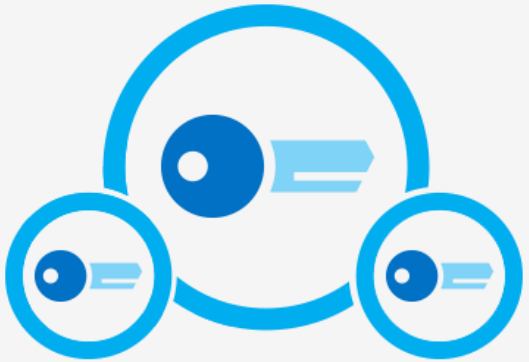


云端的TEE之Intel SGX

抗软件攻击



SGX的应用



密钥管理

区块链

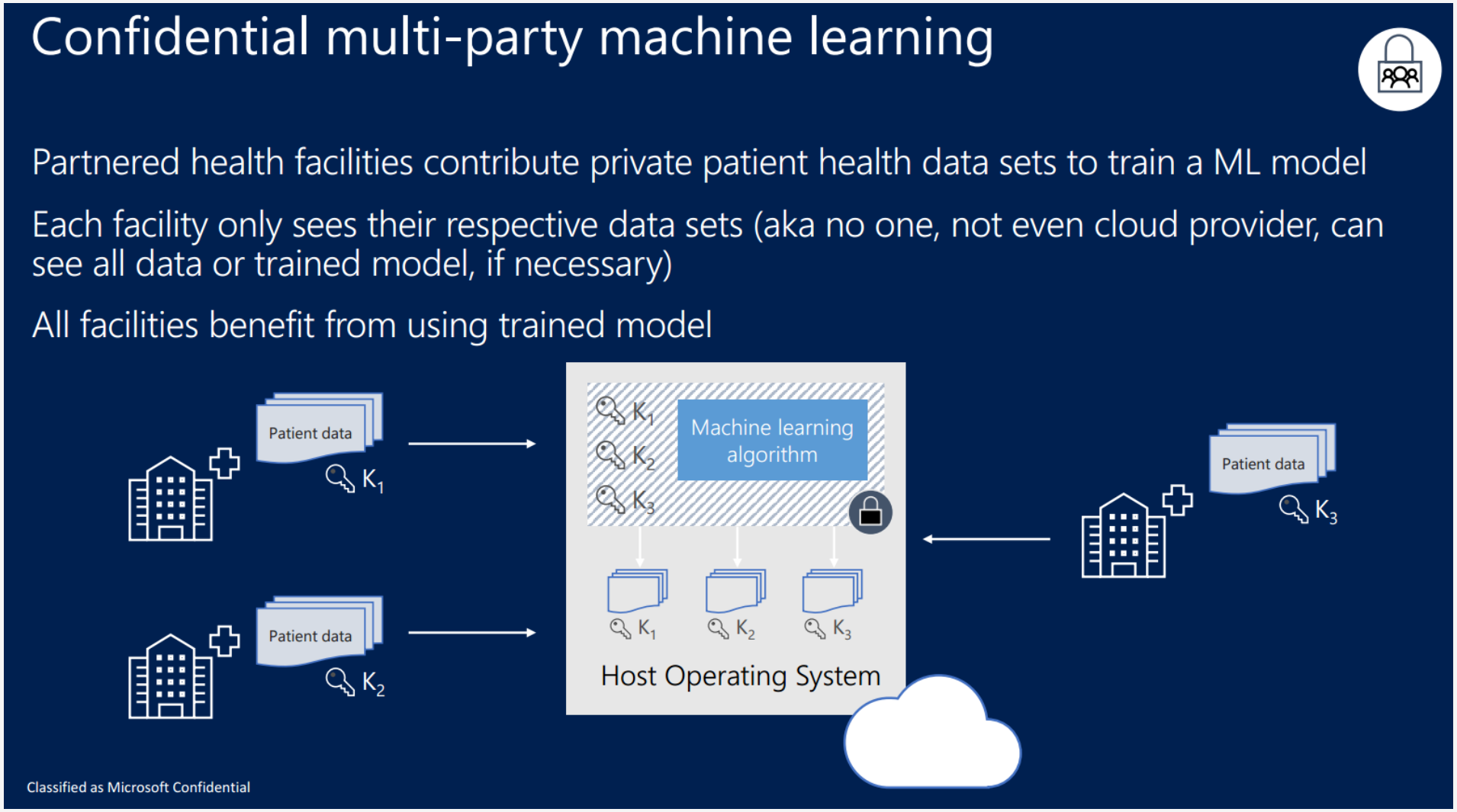
隐私计算

数字版权保护

安全通讯

数字钱包

SGX的应用


Confidential multi-party machine learning
Partnered health facilities contribute private patient health data sets to train a ML model
Each facility only sees their respective data sets (aka no one, not even cloud provider, can see all data or trained model, if necessary)
All facilities benefit from using trained model
Patient data
K1
Patient data
K2
K1
K2
K3
Machine learning algorithm
K1
K2
K3
Host Operating System
Patient data
K3
Classified as Microsoft Confidential

使用SGX需要注意哪些问题？

SGX的问题1 – 远程认证

- 远程认证的root of trust掌握在Intel公司
- 远程认证
  - ① Enclave创建及度量(软件身份)
  - ② 生成硬件签名的report
  - ③ Report发送给远程用户
  - ④ 远程用户将report转发至IAS，IAS验证report
  - ⑤ 远程用户验证软件身份
  - ⑥ 在此过程中完成基于ECDH的密钥协商

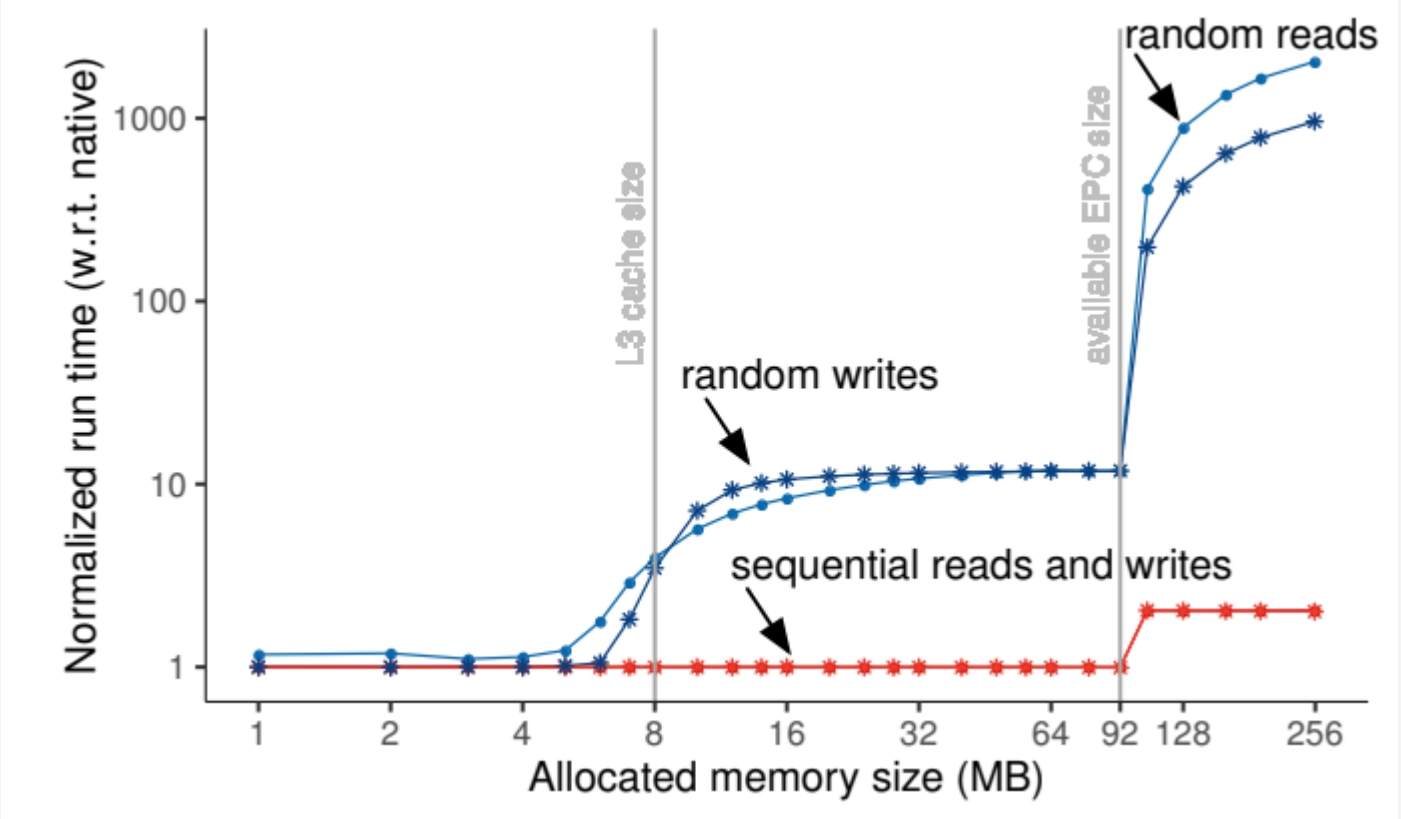
需要公开可验证的软件代码

SGX的问题2 – 抗物理/软件攻击

- 抗物理攻击目前为止没有公开发表的问题
- 抗软件攻击
  - L1TF/MDS等
  - 已得到修复(需升级最新microcode补丁，并在bios里关闭HT)

SGX的问题3 – 计算能力弱

- Enclave和普通模式切换代价高
  - 系统调用慢32倍
  - 8000 vs. 250（时钟周期）
- 内存访问代价
  - Cache miss
  - Page fault



SGX的问题3 – 计算能力弱

计算能力弱：至多8核

Product Name	Status	Launch Date	# of Cores	Max Turbo Frequency	Processor Base Frequency	Cache	TDP	Processor Graphics ‡	Compare All | None
Intel® Xeon® E-2278GEL Processor	Launched	Q2'19	8	3.90 GHz	2.00 GHz	16 MB	35 W	Intel® UHD Graphics 630	
Intel® Xeon® E-2278GE Processor	Launched	Q2'19	8	4.70 GHz	3.30 GHz	16 MB	80 W	Intel® UHD Graphics 630	
Intel® Xeon® E-2176G Processor	Launched	Q3'18	6	4.70 GHz	3.70 GHz	12 MB SmartCache	80 W	Intel® UHD Graphics 630	
Intel® Xeon® E-2186G Processor	Launched	Q3'18	6	4.70 GHz	3.80 GHz	12 MB SmartCache	95 W	Intel® UHD Graphics P630	
Intel® Xeon® Processor E3-1240L v5	Launched	Q4'15	4	3.20 GHz	2.10 GHz	8			
Intel® Xeon® Processor E3-1280 v5	Launched	Q4'15	4	4.00 GHz	3.70 GHz	8			
Intel® Xeon® Processor E3-1220 v5	Launched	Q4'15	4	3.50 GHz	3.00 GHz	8			

Intel introduced the Intel SGX Card in February 2019. It is a new way to help extend application memory protections using Intel Software Guard Extensions in existing data center infrastructure. (Credit: Intel Corporation)

Intel SGX for the Data Center

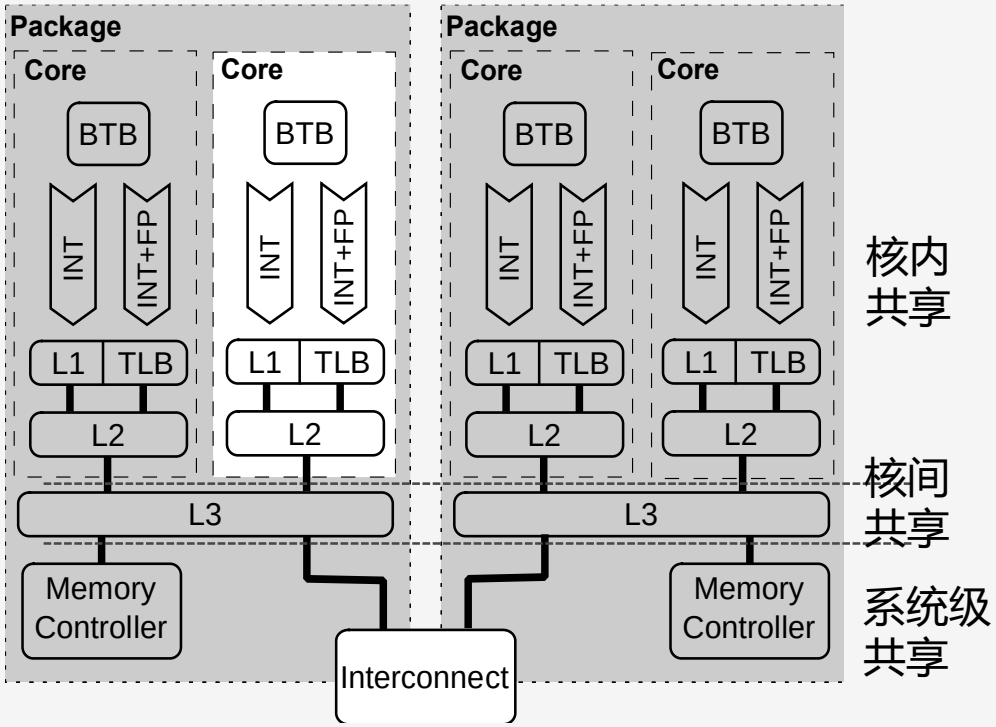
Helping protect customer data in the cloud is a top priority for cloud service providers. Intel® Software Guard Extensions (Intel® SGX) was designed to help create more secure environments without having to trust the integrity of all the layers of the system. The technology isolates specific application code and data to run in private regions of memory, or enclaves. Intel SGX is currently used by top cloud providers, including Alibaba Cloud*, Baidu*, IBM Cloud Data Guard* and Microsoft Azure* for various projects to help protect customer data at runtime. Today, Intel announced new products and ecosystem solutions that enable Intel SGX to be used even more broadly in the data center.

More: RSA 2019

Scaling Intel SGX for the Cloud: Intel introduced the Intel SGX Card, a new way to help extend application memory protections using Intel SGX in existing data center infrastructure. Though Intel SGX technology will be available on future multi-socket Intel® Xeon® Scalable processors, there is pressing demand for its security benefits in this space today. Intel is accelerating deployment of Intel SGX technology for the vast majority of cloud servers deployed today with the Intel SGX Card. Additional benefits offer access to larger, non-enclave memory spaces, and some additional side-channel protections when compartmentalizing sensitive data to a separate processor and associated cache. Availability is targeted for later this year.

SGX的问题4 – 侧信道

侧信道



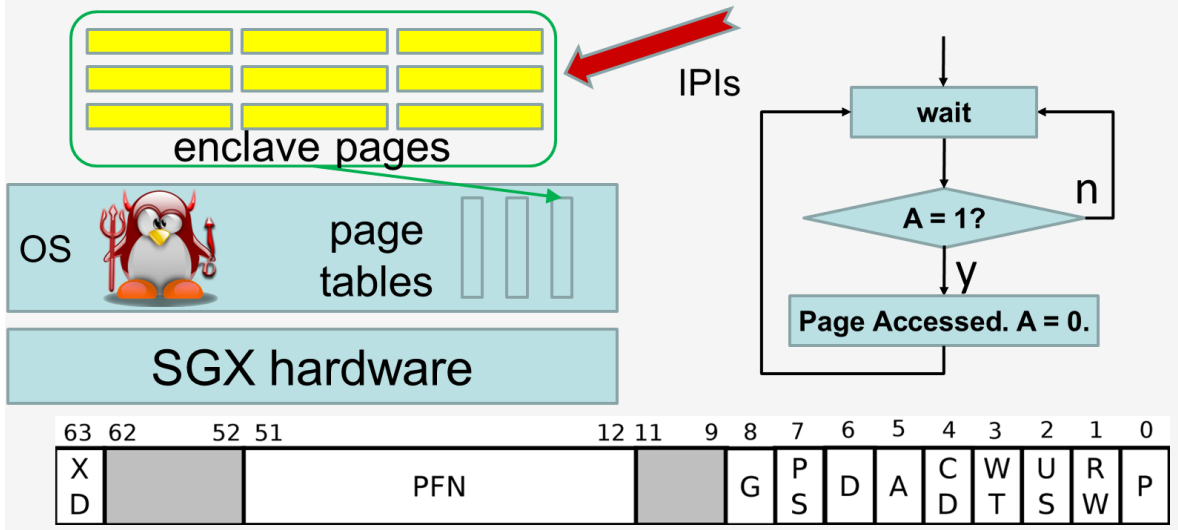
类别	示例
页表	页表项P/A/D位 [XCP,S&P'15],[BWK+,Security'17],[WCP+,CCS'17]
存储层次	多级cache、TLB、DRAM等缓存[WCP+,CCS'17]
功能单元竞争	计算单元[ABH+,S&P'19]
功能单元状态	分支预测单元[LSG+,Security'17], [ERA+,ASPLOS'18], [HMW+,CHES'20]
指令执行时间	Nemesis[BPS, CCS'18]
物理信号	电磁、功耗等

SGX的问题4 – 侧信道

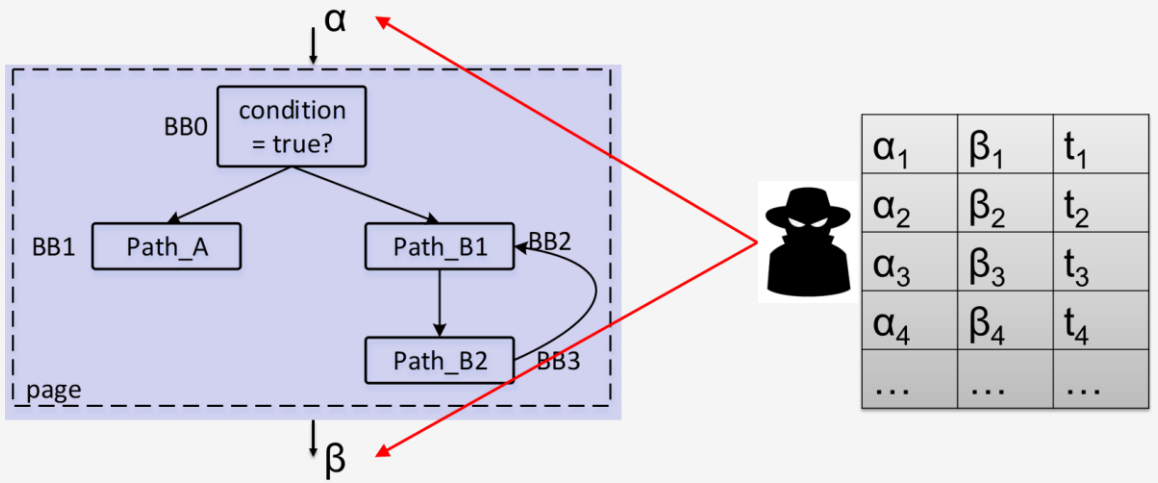
共享资源	侧信道来源或利用方式	首次由我们提出?
TLB	超线程开启时，TLB Prime + Probe 攻击方式	是
	超线程关闭时，进程切换时基于 PCID 的 TLB 选择性清空。	是
页表	触发页中断	否
	页被访问时，更新页表访问位	是
	页被修改时，更新页表修改位	是
地址翻译缓存	使用的页表项在 cache 中缓存	是
Cache	Cache是共享的	否
DRAM	内存的行缓存是共享的	否
组合攻击	时间 + 页表访问位	是
	TLB + 页表访问位	是
	Cache + DRAM 行缓存	是

SGX的问题4 – 侧信道

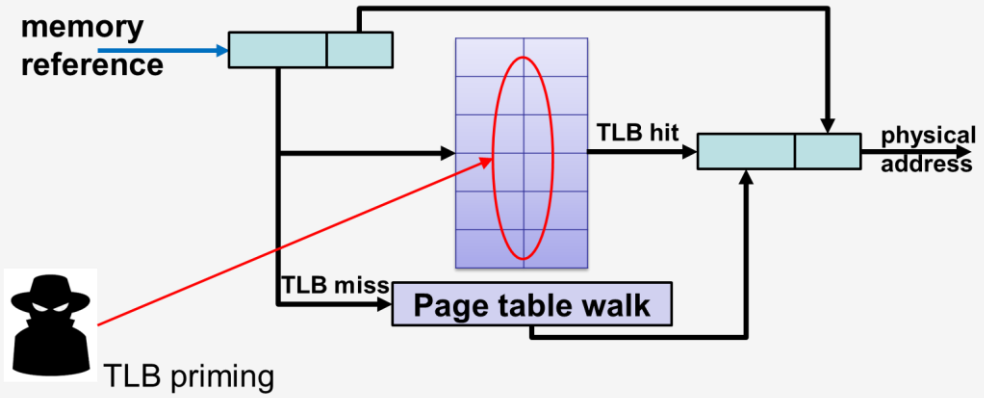
SGX 的侧信道利用可以（几乎）不触发中断



1. 被动地观察页表的访问位



2. 测量观察点之间的执行时间



3. 超线程开启时，从一个逻辑核心清空 TLB 缓存

SGX的问题4 – 侧信道

系统的角度

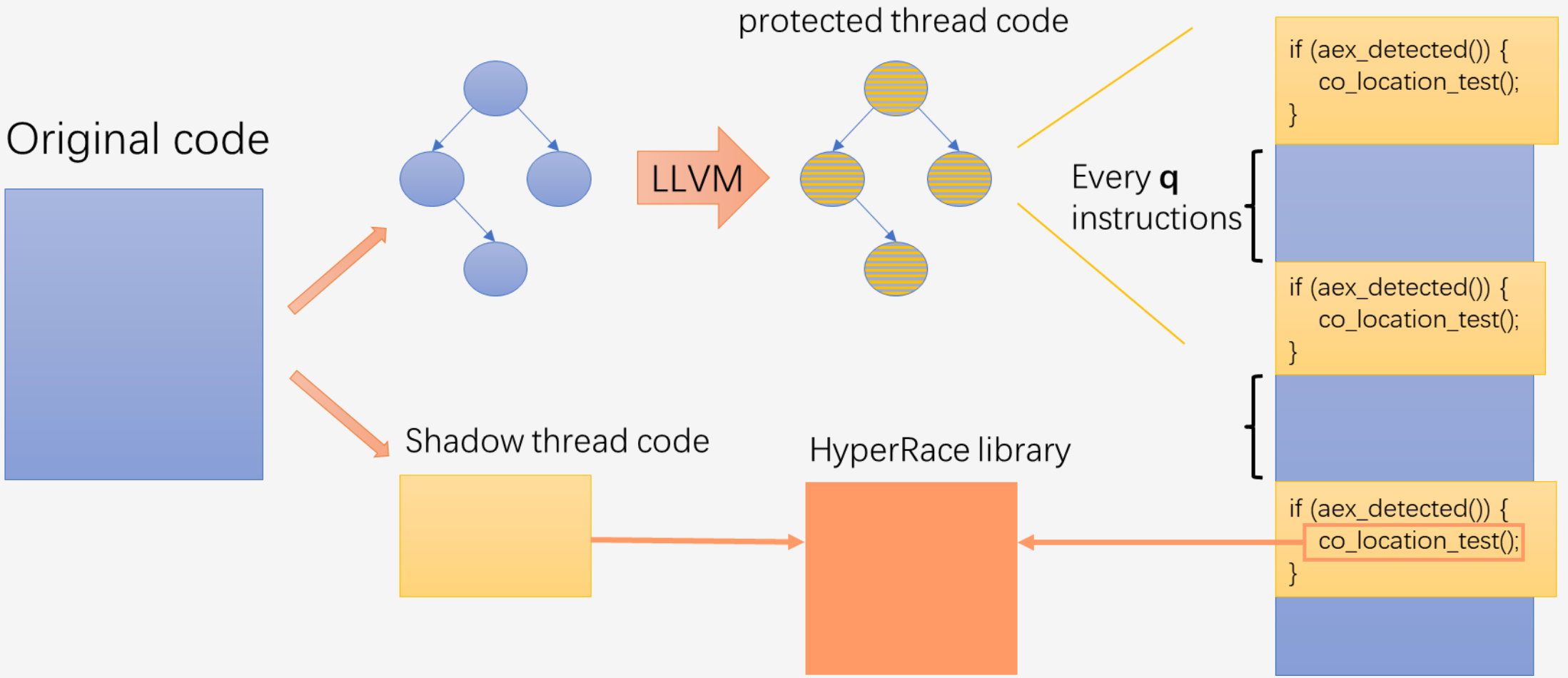
- 检测异常中断[LSK+,NDSS'17],[CZR+,AsiaCCS'17]
- 检测cache eviction[GLS+,Security'17]
- 检测中断和SMT[CWC+,S&P'18]

软件开发者的角度

- Oblivious RAM[SGW,NDSS'18], [AKS+,NDSS'18],[HOJ+,PETS'19]
- Oblivious program execution[AJX+,NDSS'19]
- 数据和代码随机化[SLK+,NDSS'17], [CKL+,ESORICS'17]

类别	子类	上下文切换时状态清空?	攻击假设或side effect	示例
同物理核攻击	功能单元状态	否	中断	BTB、BHT
		是	SMT	Store buffer、line fill buffer
	功能单元竞争		中断或SMT	L1/L2缓存、TLB、port
跨物理核攻击	三级缓存		Cache eviction	LLC
	页表		中断	页表项P位
			中断或SMT	页表项A/D位

HyperRace：消除基于中断和HT的侧信道威胁



SGX的问题4 – 侧信道

系统的角度

- 检测异常中断[LSK+,NDSS'17],[CZR+,AsiaCCS'17]
- 检测cache eviction[GLS+,Security'17]
- 检测中断和SMT[CWC+,S&P'18]

软件开发者的角度

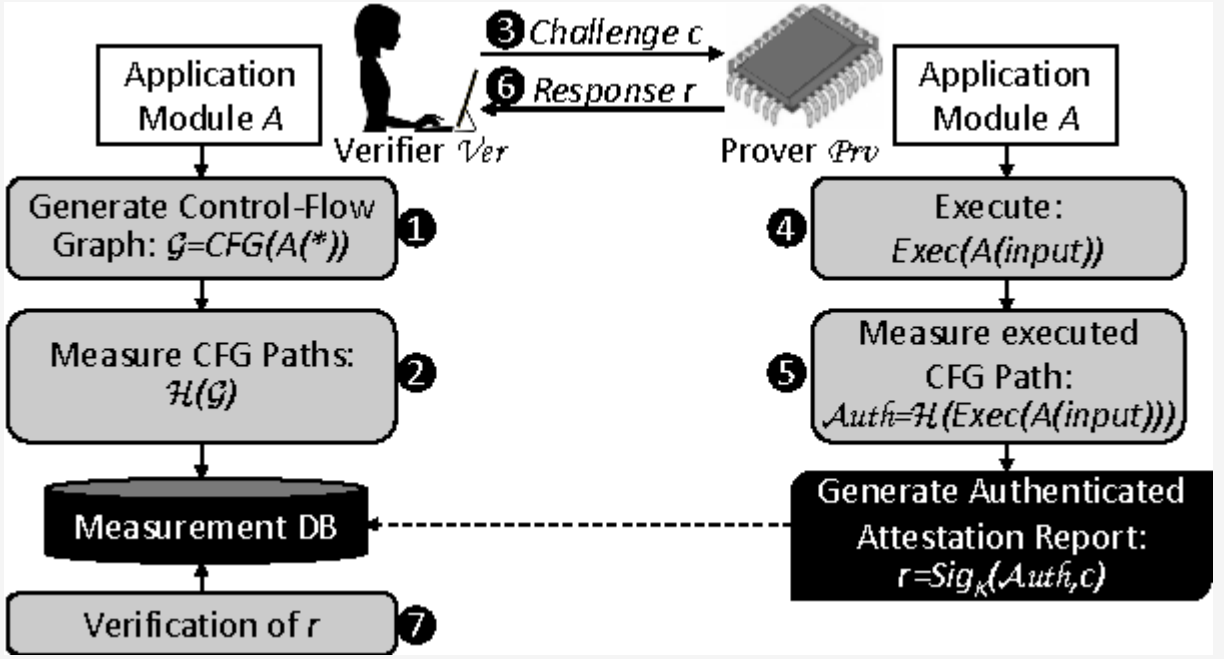
- Oblivious RAM[SGW,NDSS'18], [AKS+,NDSS'18],[HOJ+,PETS'19]
- Oblivious program execution[AJX+,NDSS'19]
- 数据和代码随机化[SLK+,NDSS'17], [CKL+,ESORICS'17]

类别	子类	上下文切换时状态清空?	攻击假设或side effect	示例
同物理核攻击	功能单元状态	否	中断	BTB、BHT
		是	SMT	Store buffer、line fill buffer
	功能单元竞争		中断或SMT	L1/L2缓存、TLB、port
跨物理核攻击	三级缓存		Cache eviction	LLC
	页表		中断	页表项P位
			中断或SMT	页表项A/D位

SGX的问题5 – 运行时状态

如何保证运行时状态的正确性？

Rust SGX SDK[WWD+,CCS'19]



Control flow attestation

SGX的问题6 – 编程和易用性

编程和易用性

- LibOS：Haven(Windows[BPH,OSDI'14])、Graphene-SGX(linux[TPV,ATC'17])、SCONE[ATG+,OSDI'16]、Occlum(蚂蚁金服)
- 程序自动分割：Glamdring(c/c++[LPM+,ATC'17])，Civet(Java[TSJ+,Security'20])
- 编程语言支持：python(MesaPy，百度)，Javascript[GWM+,Eurosec'17],GO
- 微容器：Panoply[STT+,NDSS'17]
- 中间件：Open Enclave(微软)、Asylo(Google)、SOFAEnclave(蚂蚁金服)

未来的TEE怎么设计以支持云计算等场景？

需要解决的问题

分析：应用场景对应什么需求

① 是否需要防御side channel？

② 是否需要访问IO/加速器？

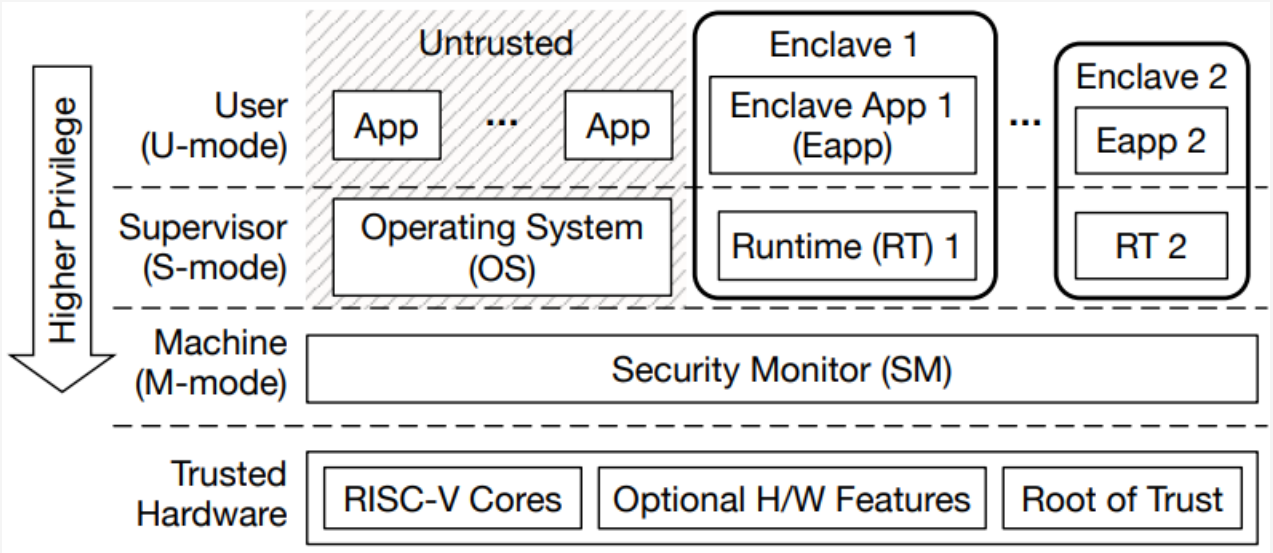
③ 抗物理攻击？

④ 计算的特点

- 高频 *vs.* 低频
- TEE的计算能力要求

Keystone Enclave

- 基于RISC-V开发
- 提供Root of Trust、驱动、SDK
- 支持内存隔离、安全启动、远程认证
- 模块化、开源、可定制的TEE
- 主要团队来自UC Berkeley

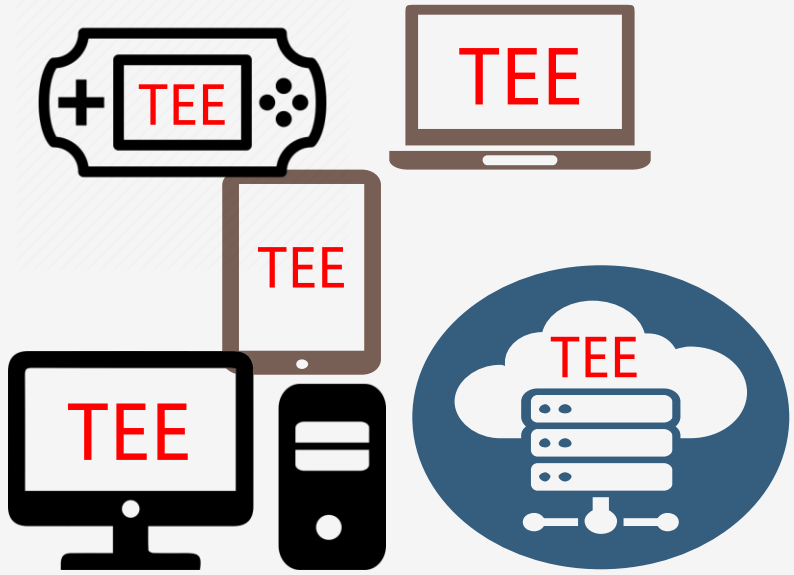


Keystone

An Open Framework for Architecting Trusted Execution Environment

总结

- 简单介绍了基于TEE实现云上的隐私计算
  - 主要是基于Intel SGX
- 学术界和工业界的一些进展
  - Google/Microsoft/阿里/百度/Intel/AMD等
- 使用TEE时，需要注意的问题
  - 侧信道/TCB/内存安全等
- 未来的TEE如何设计？



Trusted Execution Environment

谢谢！

请批评指正！

联系方式：wangwenhao@iie.ac.cn
手机：15210983075