Think in Cloud | UCLOUD | 上海交通大学 SHANGHAI JIAO TONG UNIVERSITY

START

2018 THINK IN CLOUD · BEIJING

# 安全屋 — 数据可信流通平台

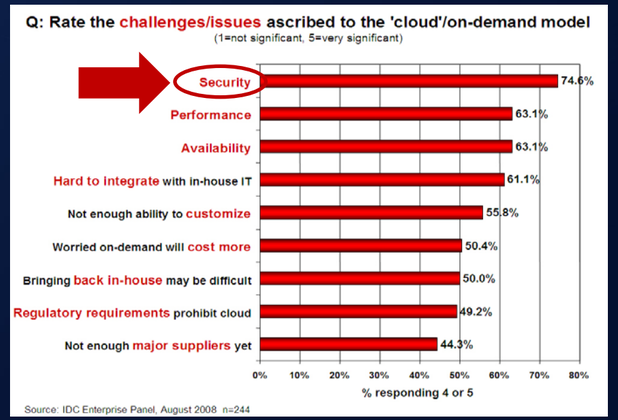
夏虞斌 · 上海交通大学副教授

1 + 1 > 2

数据的汇集产生更大的价值

# IDC-2008

安全是云计算面临的首要挑战



## IDC-2017

安全依然是云计算面临的主要问题

“Recently enterprises are increasingly becoming the targets of hackers as the digital transformation boosts their digital asset value, making security a major concern for public cloud service tenants.”

https://www.idc.com/getdoc.jsp?containerId=prCHE43003117

# 云是否一定需要用户数据明文?

**不需要明文的例子**

- 云存储：Dropbox、百度盘等
- 用户将加密后的数据发送至云服务商保存

**需要明文的例子**

- 大数据分析、数据训练等
- 对数据进行运算时，必须在内存中解密数

## 如何降低对云的安全依赖?

- 依赖-1：所有管理员均为可信
- 依赖-2：攻击者无法接触硬件设备
- 依赖-3：云端的软件设计均为安全
- 依赖-4：云端的硬件设备均为安全
- 依赖-5：云端的CPU是安全的

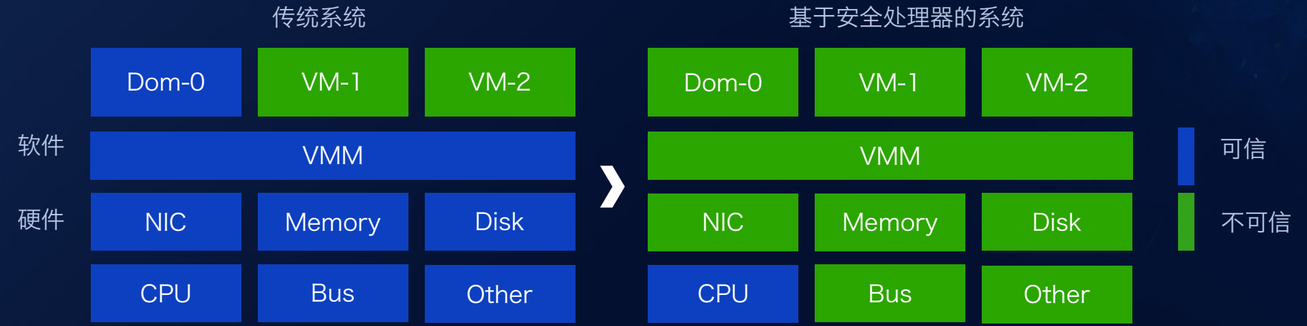
# 安全CPU

**降低对云提供商的信任依赖**

不信任内存、硬盘、网卡等外部设备

只信任安全处理器，可抵御物理攻击

服务器无需数据明文，依然可管理资源



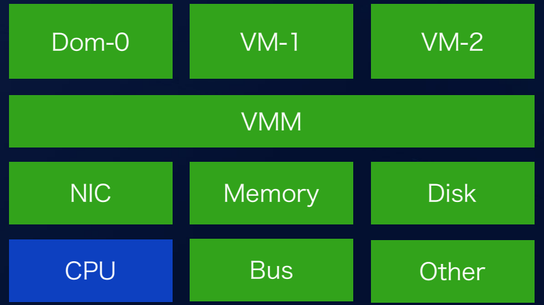
# TEE

可信执行环境（Trusted Execution Environment）

基于CPU硬件安全扩展，且与外部完全隔离的执行环境

通过远程认证进行身份识别，获取运行Key后加密执行

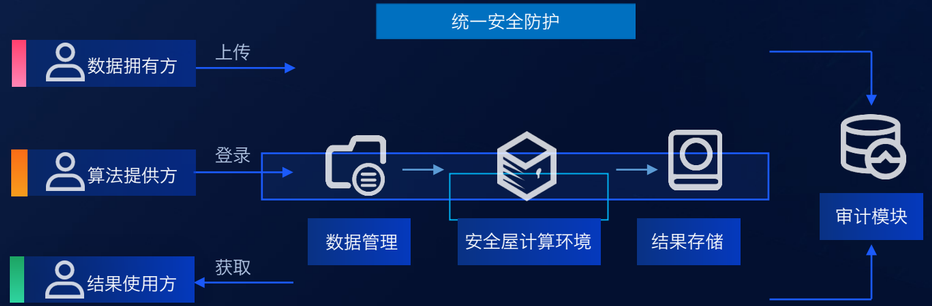
软硬件结合的安全增强方案，抵御各类侧信道攻击



# TEE+安全屋

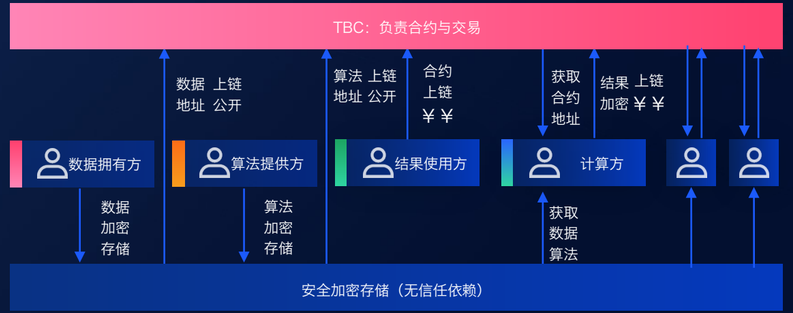
## 最小化对云端安全屋的信任依赖

数据拥有方、算法提供方、结果使用方、计算提供方
算法在TEE中完成对数据的访问与运算，明文不外泄



# TEE+区块链+安全屋

- 分布式的可信数据运算
- 公有链平台的私有智能合约
- 智能合约通过TEE保护执行
- 基于硬件保护合约代码和数据
- 可直接对接以太坊




ShadowEth: Private Smart Contract on Public Blockchains, [JCST-18]

# 四大特点


全球任何计算节点
均可接入计算框架


单一信任模型→
分布式信任模型


计算节点无法
泄露计算数据


TEE中运行计算
可无缝在线迁移

2018 THINK IN CLOUD · BEIJING

# Intel® SGX (Software Guard Extensions) 简介

王立刚 Intel中国首席平台安全架构师

# Intel® SGX：面向所有开发者的应用级TEE

SGX 为程序的敏感代码和数据提供了安全空间


恶意代码不能访问目标程序的敏感数据

敏感数据受SGX enclave保护

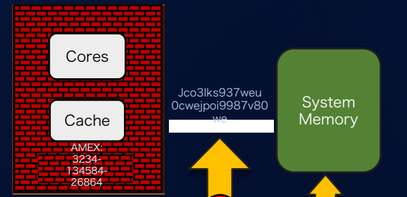
需要一个保险箱及相关防护

Intel 硬件构成了SGX的底层基础

SGX程序被分为了两部分：可信部分和不可信部分

可信部分受加密内存保护

CPU 封装

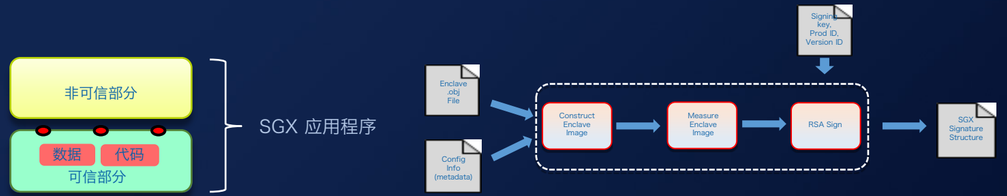


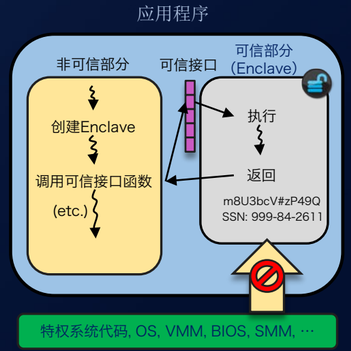
# Intel® SGX：
# 面向所有开发者的应用级TEE

Intel® SGX 使应用程序可以创建自己的TEE，并且决定把哪些代码和数据放入TEE保护，给与了应用开发者对应用安全直接的控制。

把可信计算基（Trusted Computing Base）减小到最小，从而把受攻击风险降到最低
防止软件攻击，即使OS/drivers/BIOS/VMM/SMM层面已被攻破
即使攻击者控制了整个系统，敏感数据依然受到保护
防止内存总线监听、篡改、和冷启动攻击
提供基于硬件的程序认证
在主CPU上运行，充分利用Intel处理器的性能优势

# SGX应用开发与执行



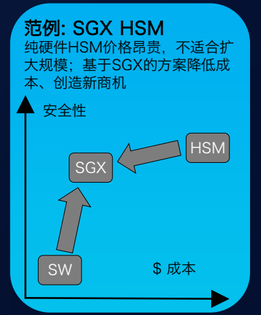

- 应用程序被分为可信和非可信两部分
- App程序首先进入非可信部分，创建enclave即可信部分，可信部分位于加密内存
- 可信接口函数被调用；Enclave内的数据，Enclave内代码看到的是原文，而Enclave外对它的访问是禁止的
- 函数返回；Enclave数据仍在加密内存中

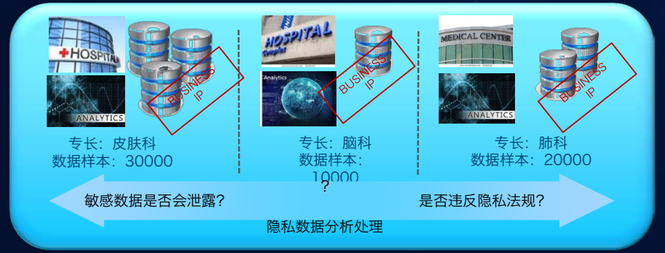
# SGX在云/服务器端应用

**云计算**
- SSL服务器保护
- Per-host密钥管理
- Map/Reduce加固
- 敏感大数据分析的隐私隔离

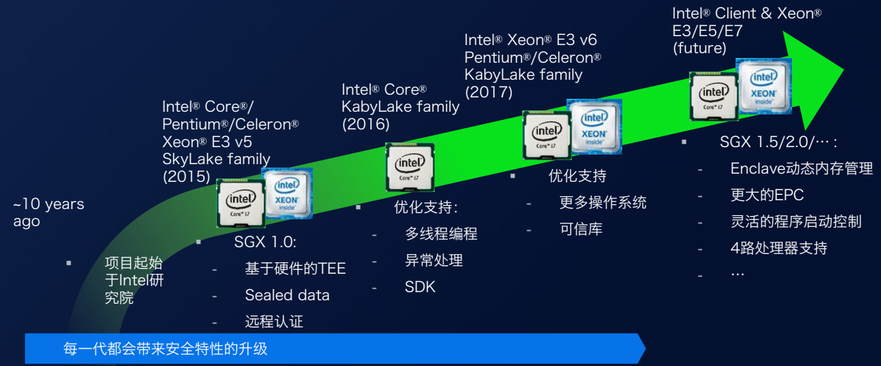
**电信**
- Per-host key密钥管理
- NFV环境中保护管理白名单

**企业**
- 加密数据库操作，保护内存常驻数据和查询
- SSL服务器保护
- Per-host密钥管理
- 敏感大数据分析的隐私隔离
- 提供对嵌入式应用和设备的防篡改解决方案



# SGX历史回顾及未来展望



# THANKS