硬件安全问题及防护

王文浩

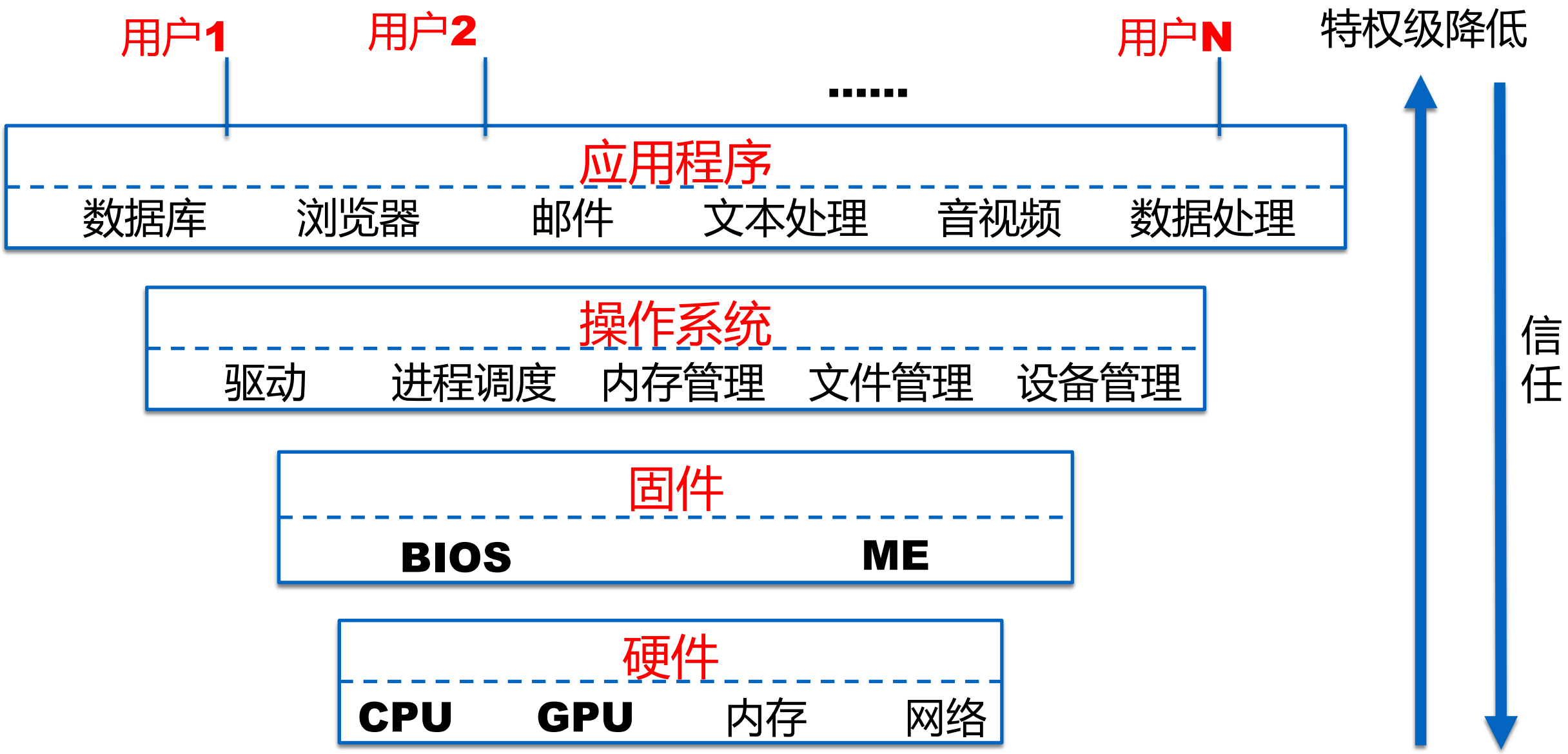
2020年12月

"All problems in computer science can be solved by another level of indirection." by David Wheeler

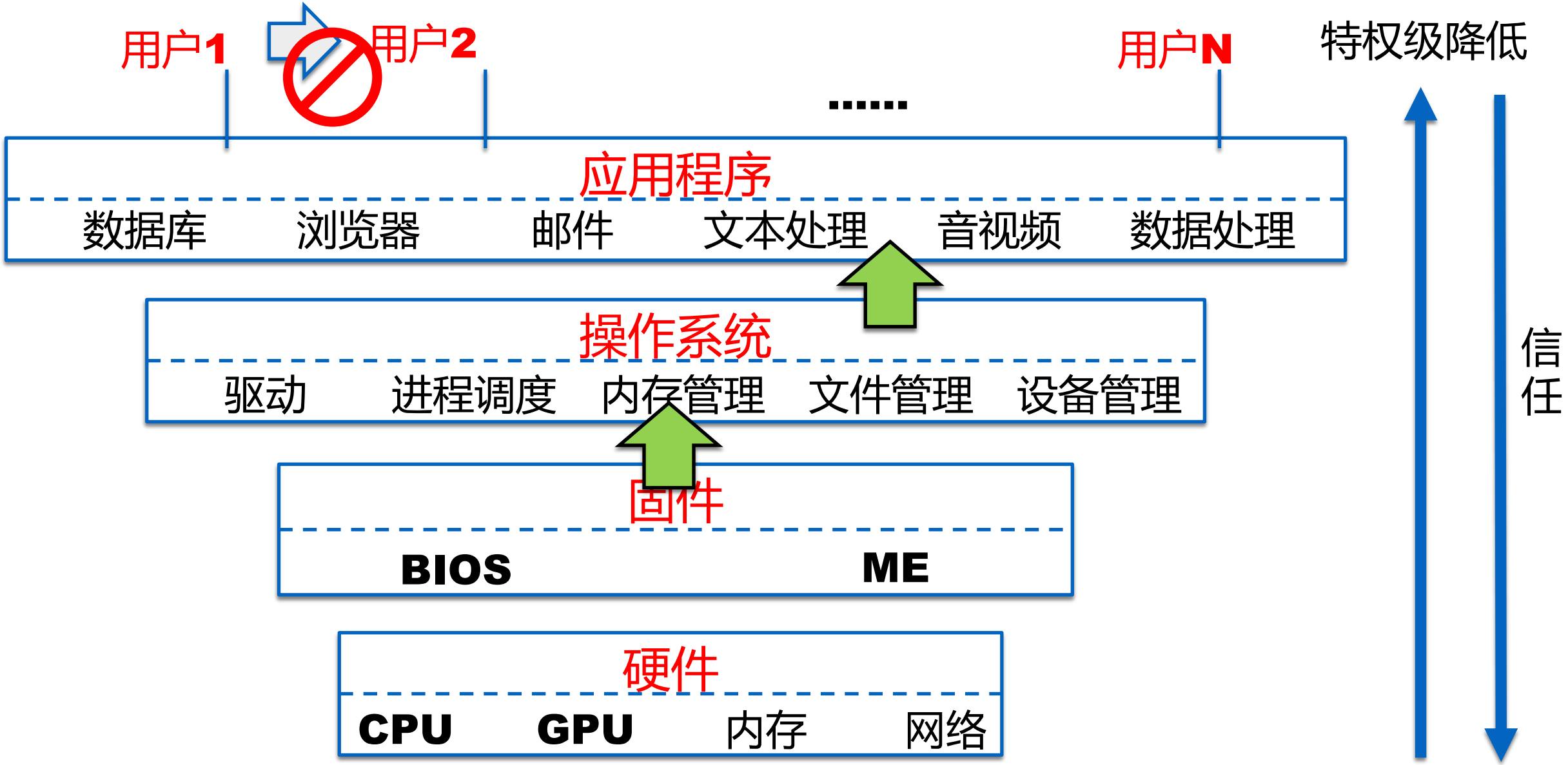
... except for the problem of too many layers of indirection.

layers of indirection ⟷ *abstraction layer*

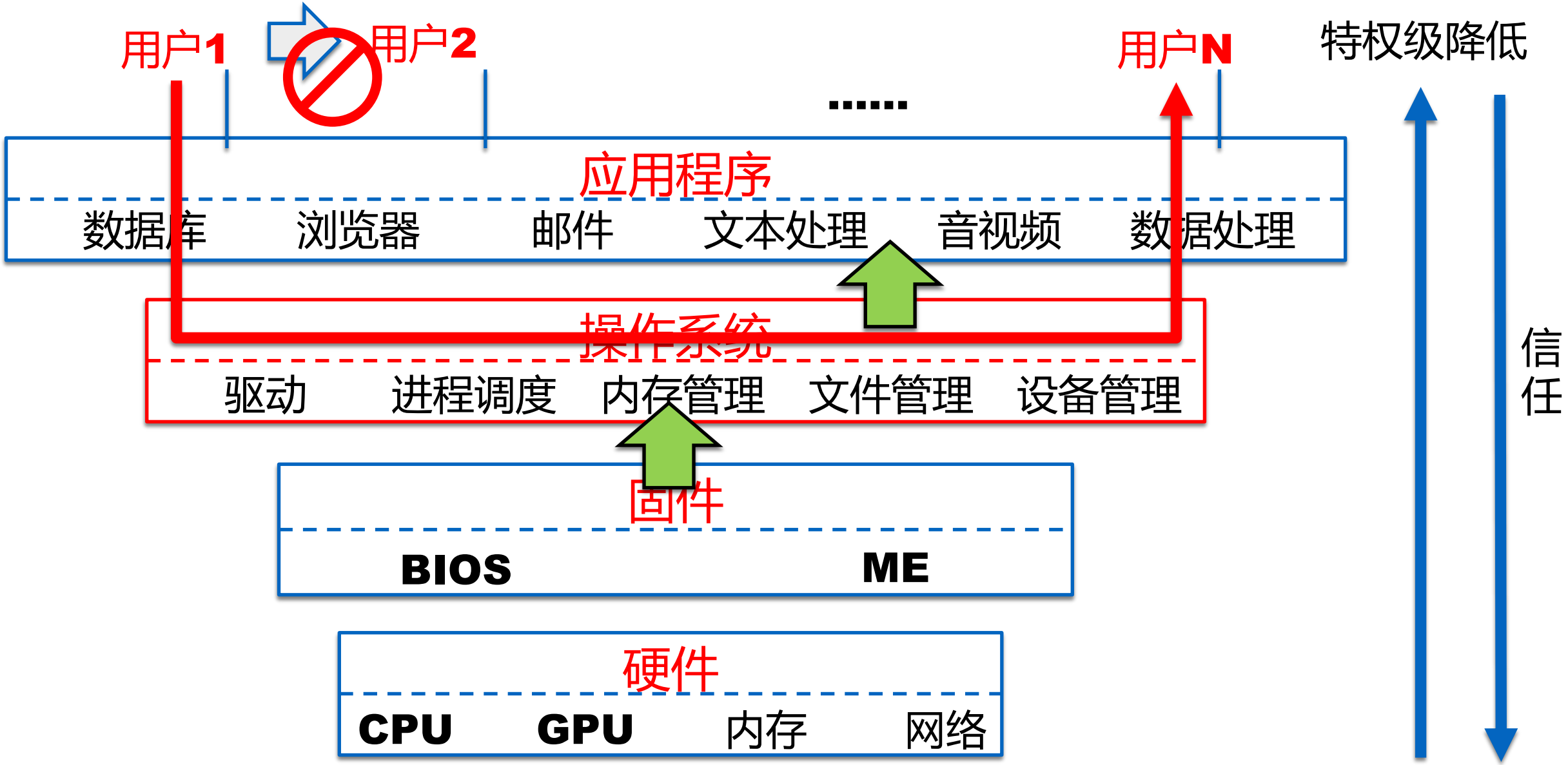
计算机系统


用户1
用户2
.....
用户N
特权级降低
应用程序
数据库
浏览器
邮件
文本处理
音视频
数据处理
操作系统
驱动
进程调度
内存管理
文件管理
设备管理
固件
BIOS
ME
硬件
CPU
GPU
内存
网络
信任

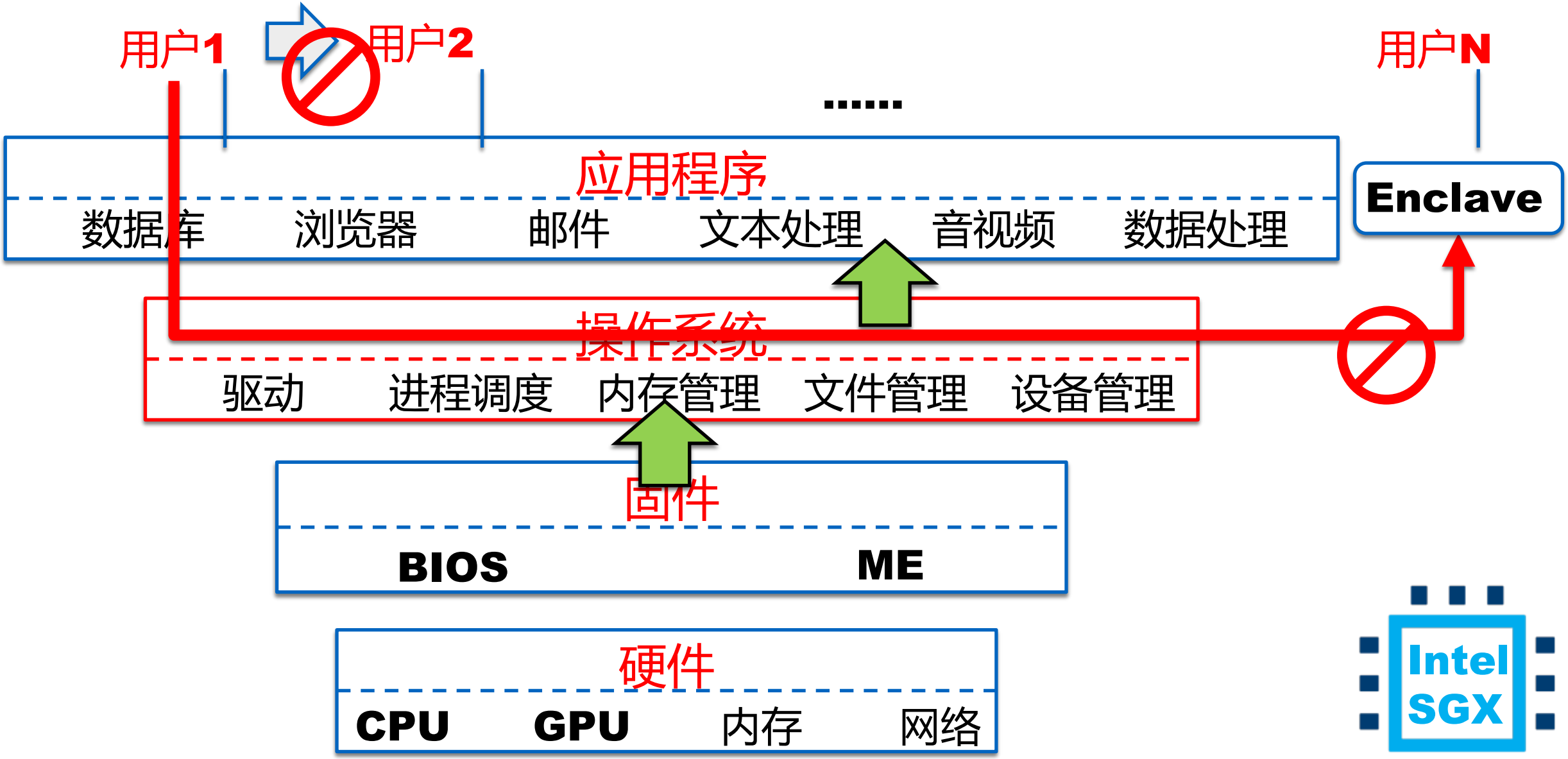
计算机系统


用户1
用户2
.....
用户N
特权级降低
应用程序
数据库
浏览器
邮件
文本处理
音视频
数据处理
操作系统
驱动
进程调度
内存管理
文件管理
设备管理
固件
BIOS
ME
硬件
CPU
GPU
内存
网络
信任

当操作系统不可信时。。。


用户1
用户2
.....
用户N
特权级降低
应用程序
数据库
浏览器
邮件
文本处理
音视频
数据处理
操作系统
驱动
进程调度
内存管理
文件管理
设备管理
固件
BIOS
ME
硬件
CPU
GPU
内存
网络
信任

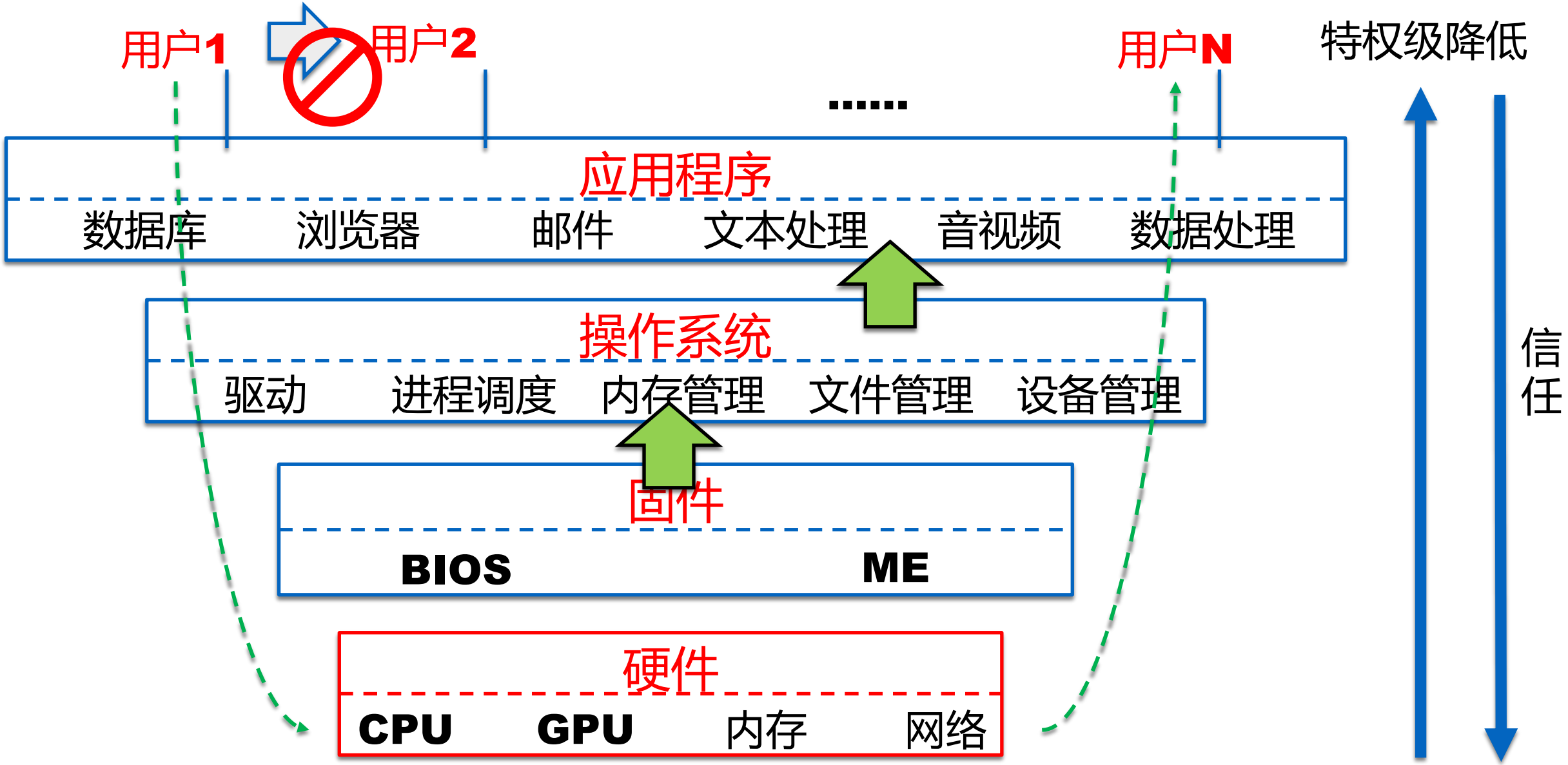
当操作系统不可信时。。。


用户1
用户2
.....
用户N
应用程序
数据库
浏览器
邮件
文本处理
音视频
数据处理
Enclave
操作系统
驱动
进程调度
内存管理
文件管理
设备管理
固件
BIOS
ME
硬件
CPU
GPU
内存
网络
Intel
SGX

OS等系统软件不可信

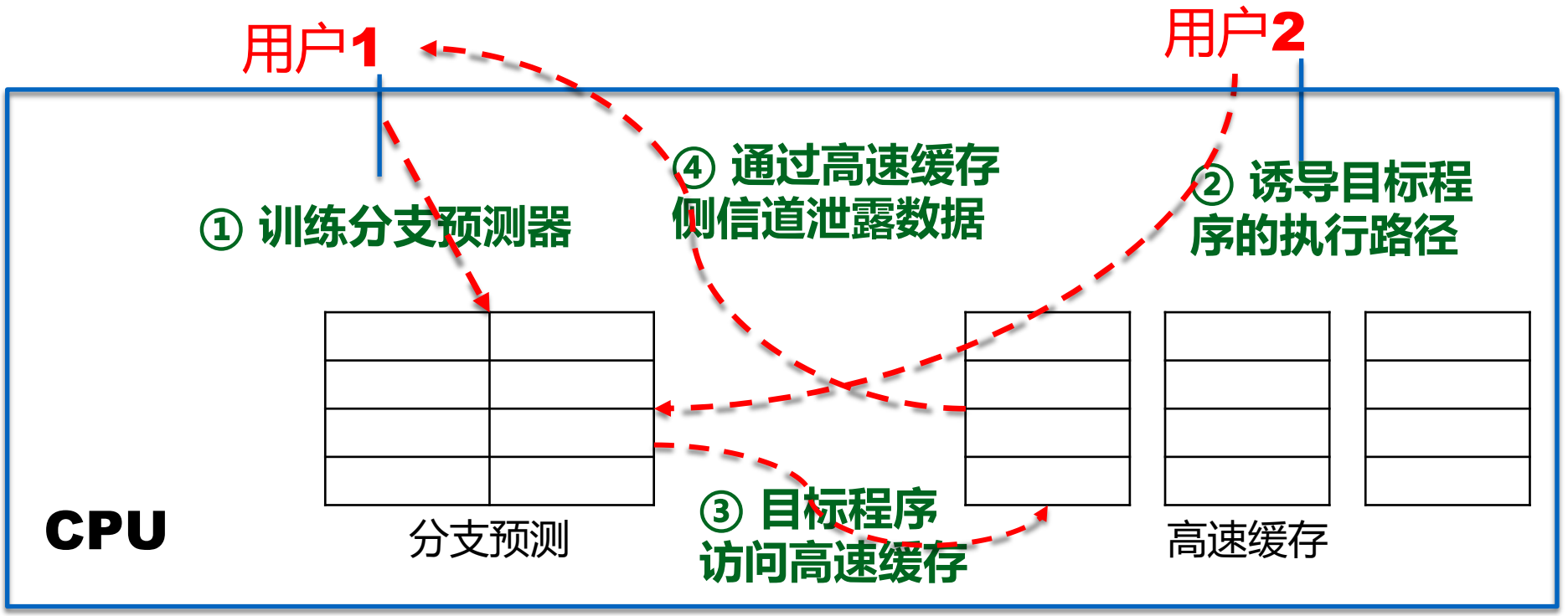
- 可信执行环境 (TEE)
  - Intel SGX，AMD SEV，ARM TrustZone，keystone enclave等
  - TCB仅包含CPU和TEE代码本身
  - 攻击者可以拥有操作系统等特权级代码执行权限
- 隐私计算

但是，当底层硬件出现问题时



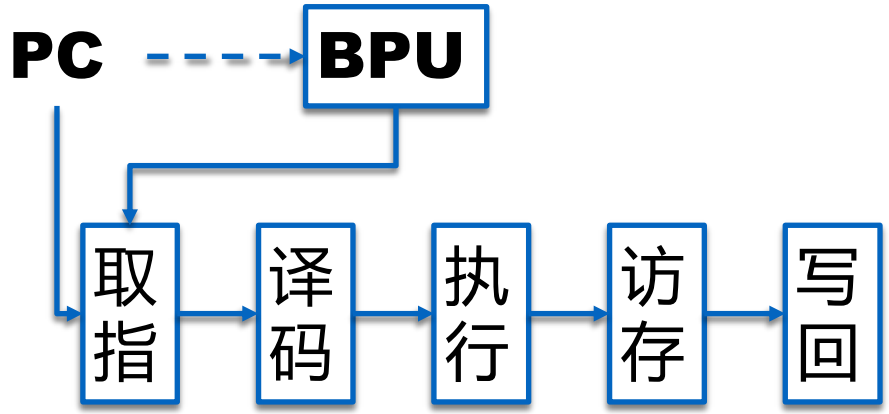
底层硬件问题 -- CPU

- 侧信道攻击
  - 根本原因是硬件资源的共享使用及竞争
- CPU：微体系结构侧信道
  - 幽灵（Spectre）



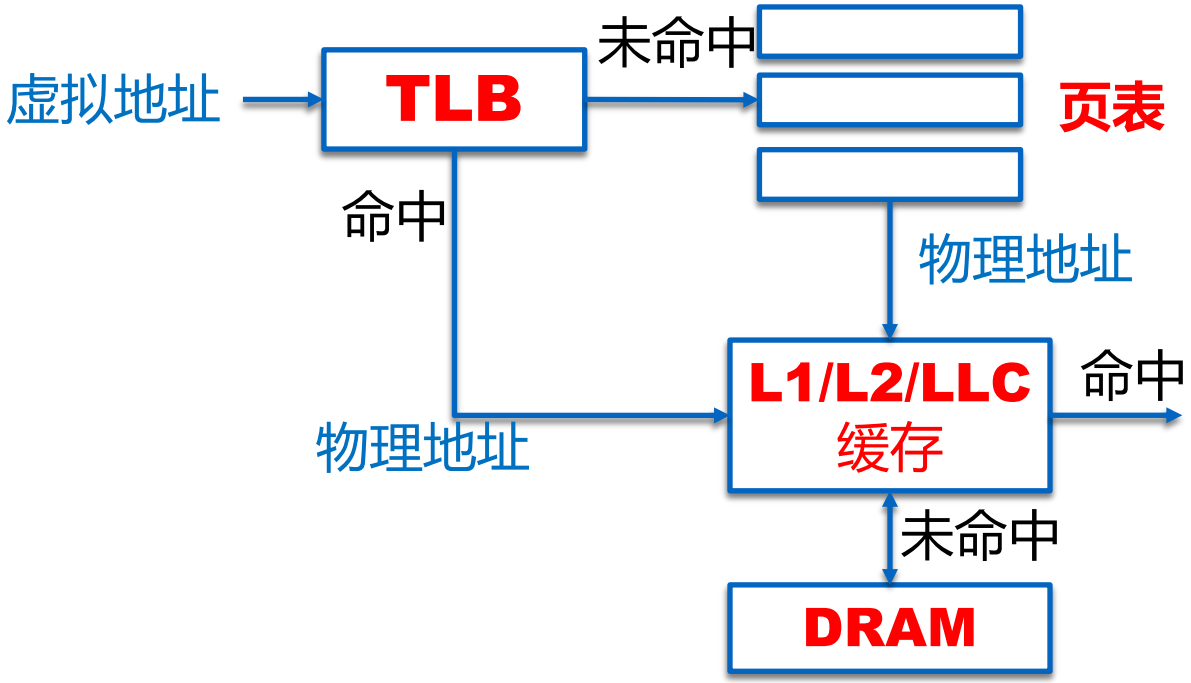
CPU微体系结构侧信道

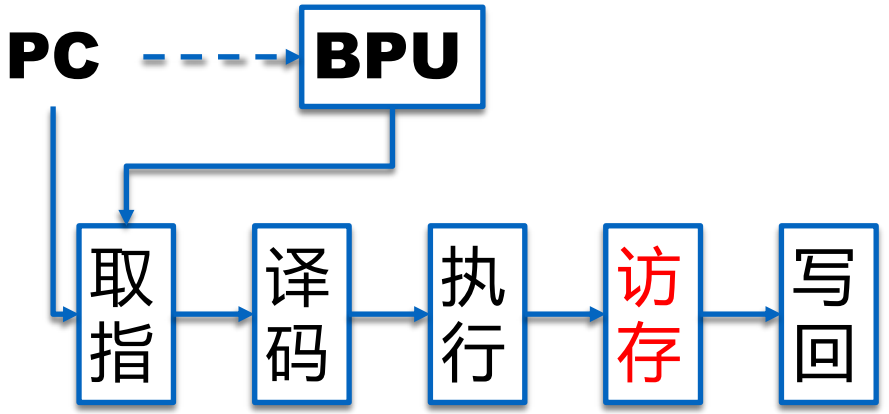
- CPU -- 可信执行环境 (TEE)
  - Intel SGX，AMD SEV，ARM TrustZone，keystone enclave等



CPU微体系结构侧信道

- CPU -- 可信执行环境 (TEE)
  - Intel SGX，AMD SEV，ARM TrustZone，keystone enclave等
- 针对Intel SGX的侧信道攻击
  - 访存过程的侧信道[1]

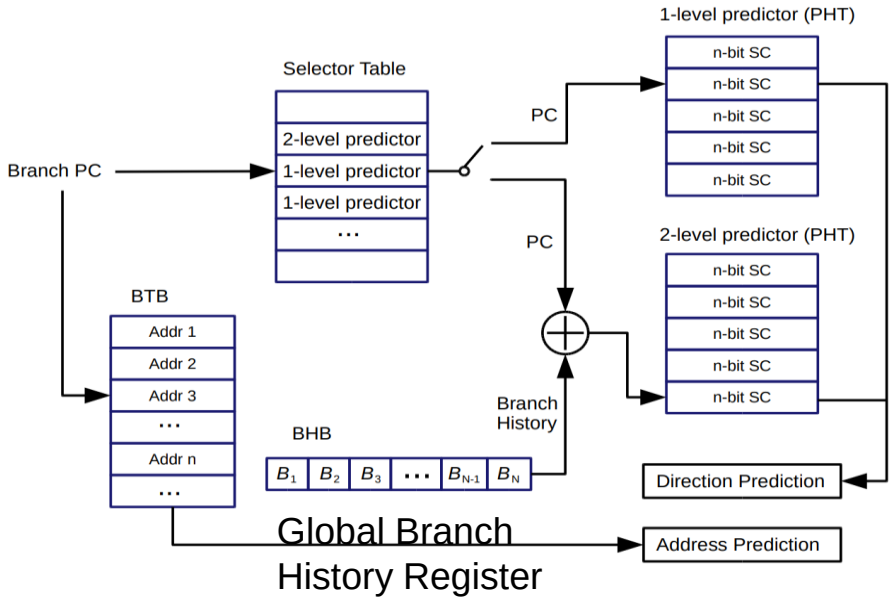


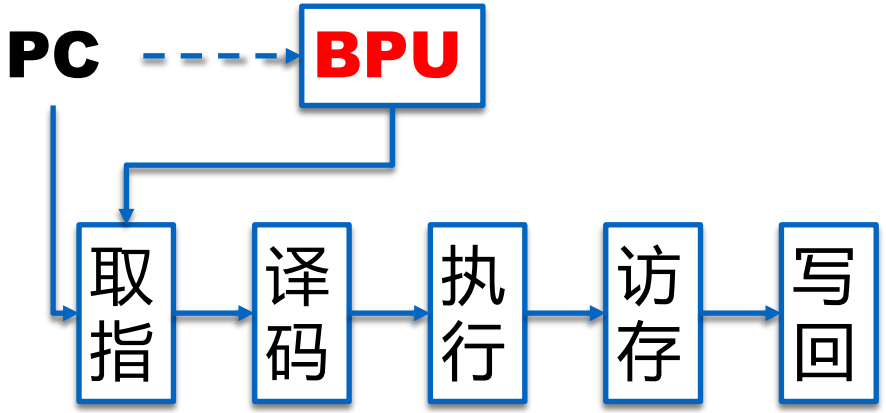


[1] Leaky Cauldron on the Dark Land: Understanding Memory Side-Channel Hazards in SGX. CCS 2017

CPU微体系结构侧信道

- CPU -- 可信执行环境 (TEE)
  - Intel SGX，AMD SEV，ARM TrustZone，keystone enclave等
- 针对Intel SGX的侧信道攻击
  - 访存过程的侧信道[1]
  - 分支预测过程中的侧信道[2]





[2] Bluethunder: A 2-level Directional Predictor Based Side-Channel Attack against SGX. CHES 2020

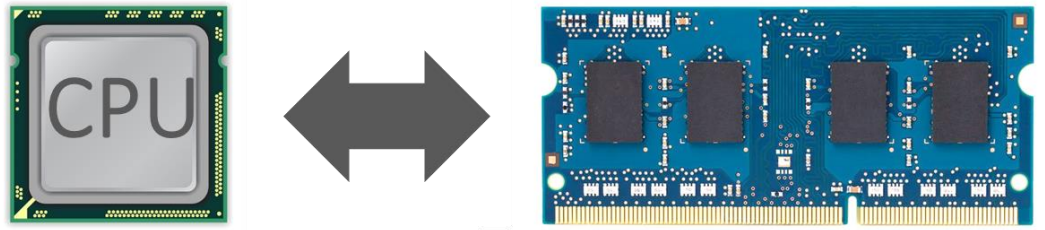
CPU微体系结构侧信道

- CPU -- 可信执行环境 (TEE)
  - Intel SGX，AMD SEV，ARM TrustZone，keystone enclave等
- 针对Intel SGX的侧信道防御
  - 纯软件手段的资源隔离：防御基于超线程和/或中断的侧信道攻击--HyperRace[3]
  - 借助硬件的资源隔离：可有效防御侧信道的新型异构TEE设计--HETEE[4]
  - 防御侧信道的新型高速缓存设计[5]

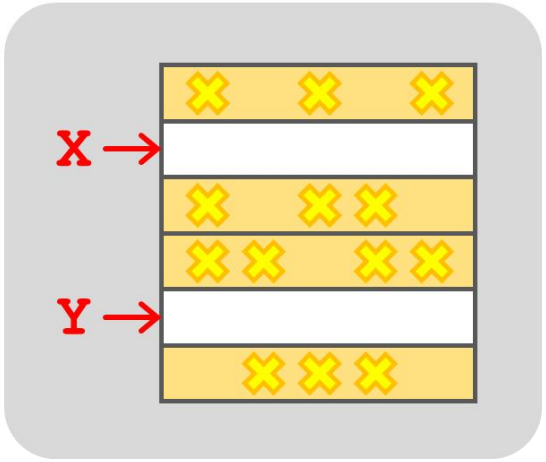
[3] Racing in Hyperspace: Closing Hyper-Threading Side Channels on SGX with Contrived Data Races. S&P 2018
[4] Enabling Rack-scale Confidential Computing using Heterogeneous Trusted Execution Environment. S&P 2020
[5] Randomized Last-Level Caches Are Still Vulnerable to Cache Side-Channel Attacks! But We Can Fix It. S&P 2021

底层硬件问题 – 内存

- 侧信道攻击
  - 根本原因是硬件资源的共享使用及竞争
- 内存：Rowhammer
  - 系统提权
  - 沙盒逃逸
  - 神经网络攻击
- 目前DRAM的硬件防御机制
  - TRR
  - ECC




```
loop:
  mov (X), %eax
  mov (Y), %ebx
  clflush (X)
  clflush (Y)
  mfence
  jmp loop
```



Rowhammer攻防

- Rowhammer的成功率和哪些因素有关？[6]
  - Hammer模式
  - 数据模式
  - True/anti cell
  - DDR3/DDR4/TRR/厂商?
- 防御
  - 基于软件的TRR (target row refresh)技术[7]

[6] BitMine: An End-to-End Tool for Detecting Rowhammer Vulnerability. In submission to TIFS
[7] Protect Page Tables Against RowHammer Attacks using Software-only Target Row Refresh. In submission to ATC 2021

总结、展望

- CPU
  - 侧信道对网络系统、云计算、浏览器、终端设备等的威胁
  - 理解CPU漏洞的根源：资源共享、乱序执行、分支预测?
  - 安全体系结构设计和防御技术
- 内存
  - rowhammer对浏览器沙盒、云计算平台（ECC）的实际威胁程度
- 其它硬件和固件组件
  - Intel ME/GPU/FPGA/AI/ARM/RISC-V
- 基于硬件机制的系统设计
  - Intel MPK/TDX等
- 硬件安全问题的困难
  - 公开信息少
  - 硬件修补、迭代慢

谢谢聆听！