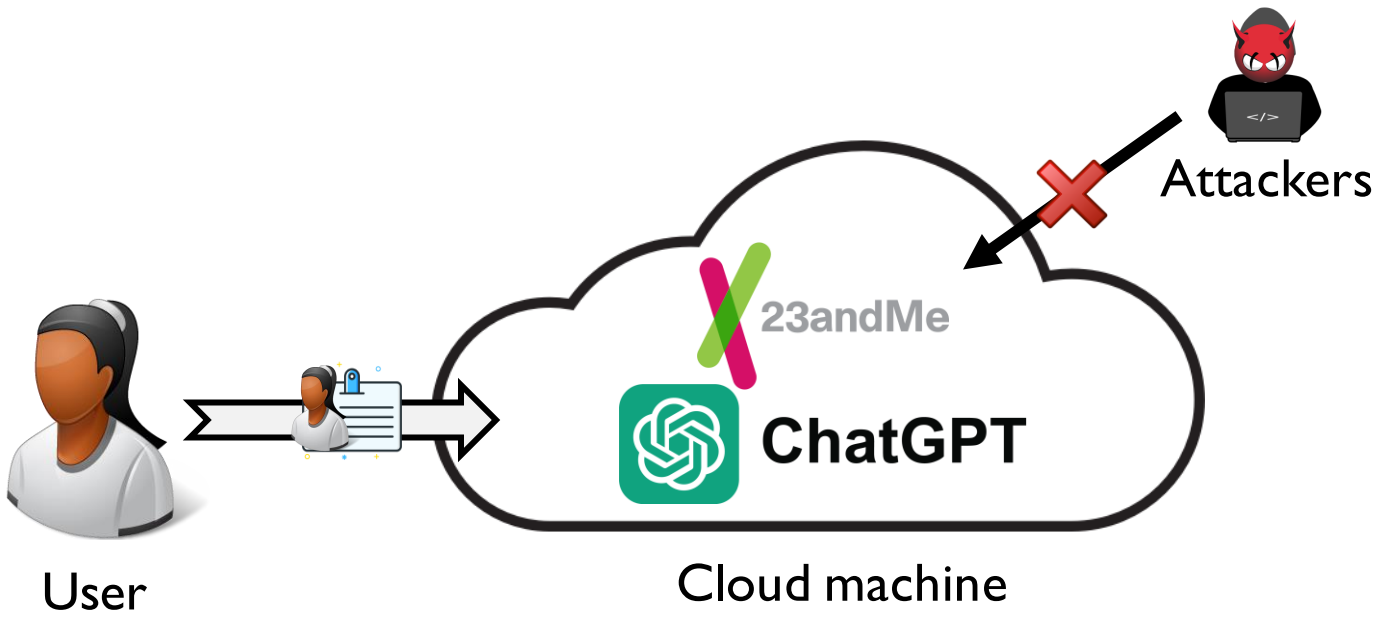
An Extensible Orchestration and Protection Framework for Confidential Cloud Computing

Adil Ahmad, Alex Shultz, Byoungyoung Lee, and Pedro Fonseca

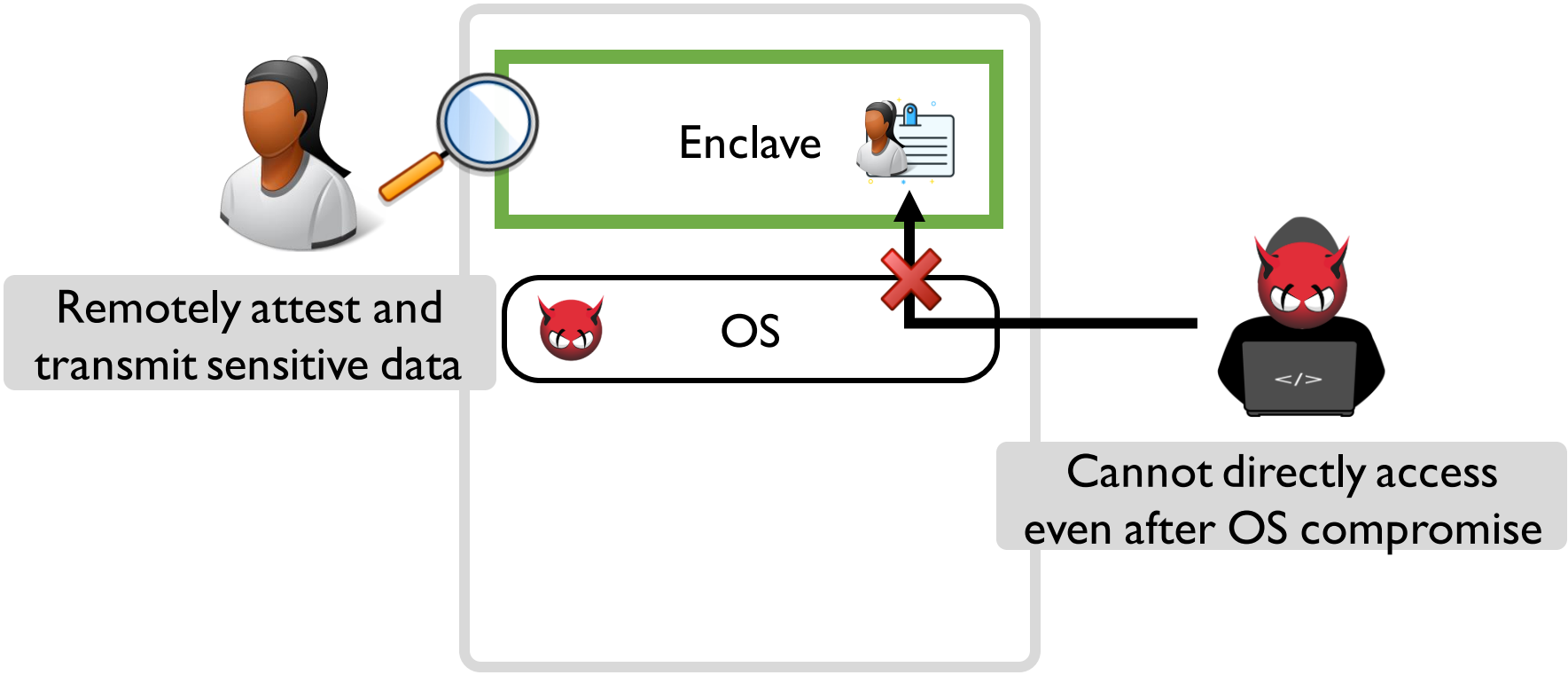
서 울 대 학 교
SEOUL NATIONAL UNIVERSITY

Confidentiality of data in cloud machines is *critical*



Many cloud providers leverage *SGX* for confidentiality

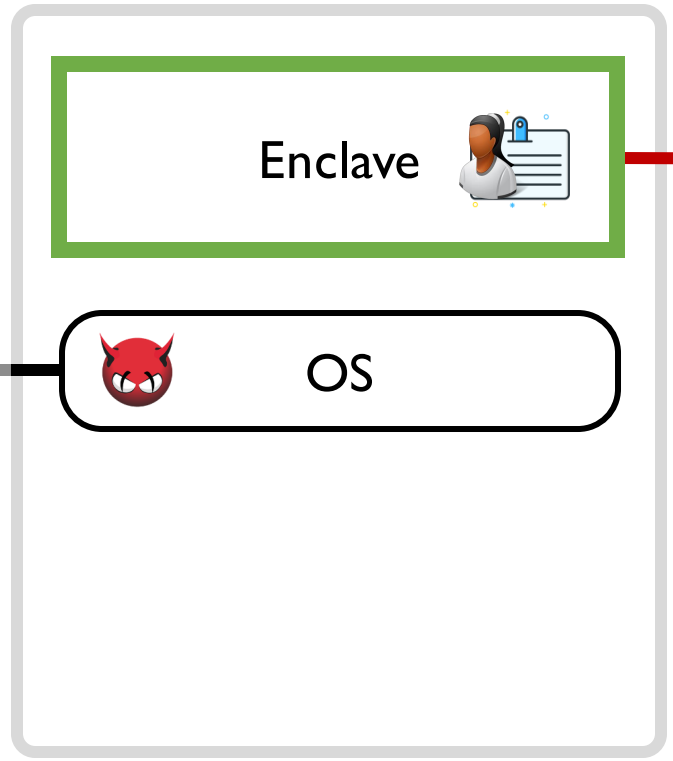
IBM Cloud Microsoft Azure Alibaba Cloud



SGX *lacks features* required by providers and users

- Enclave usage billing
- Prevent malware loading

No secure orchestration:
providers rely on untrusted OS

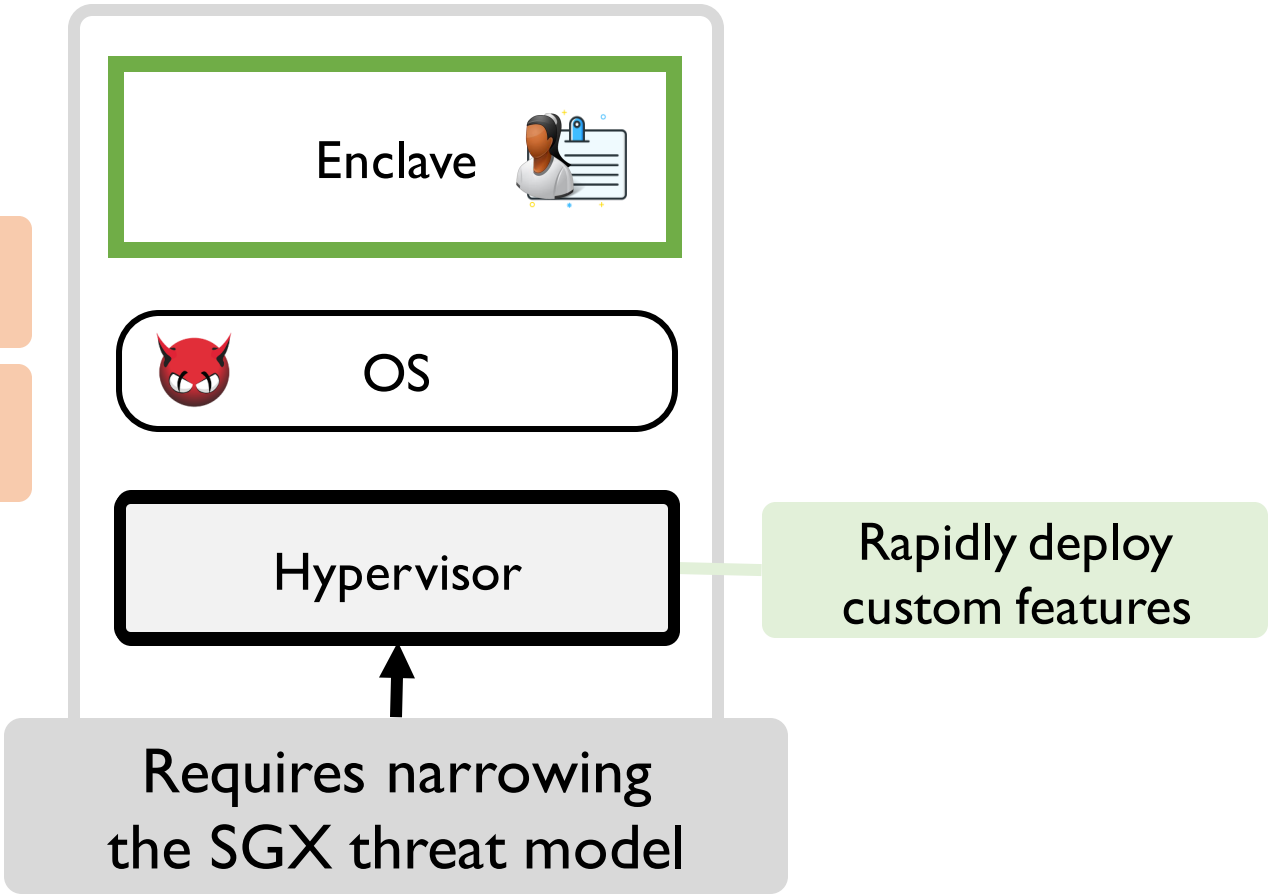


Side-channels

No side-channel defense
against the OS

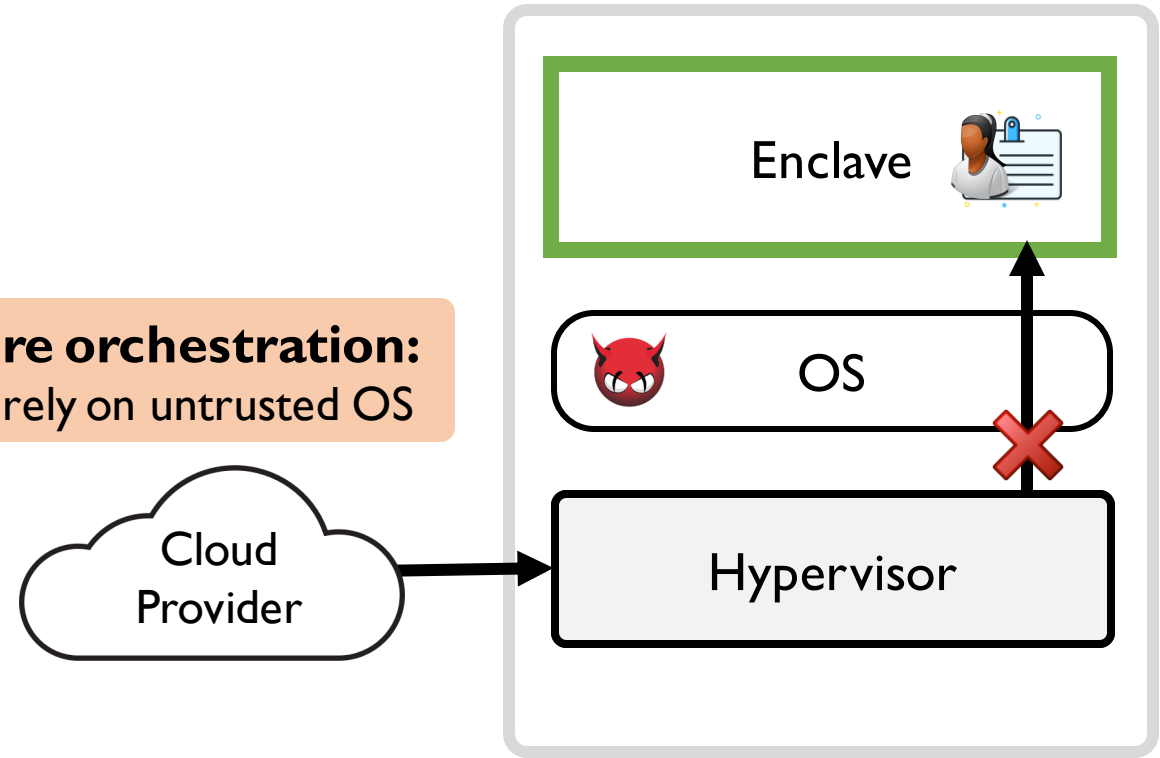
Waiting for CPU updates is *not an option*

- **Slow**
  SGX1→SGX2 took 5 years
- **Uncertain**
  Side-channels known for 20 years



Can we realistically narrow the threat model?

Yes, for our specific use-cases

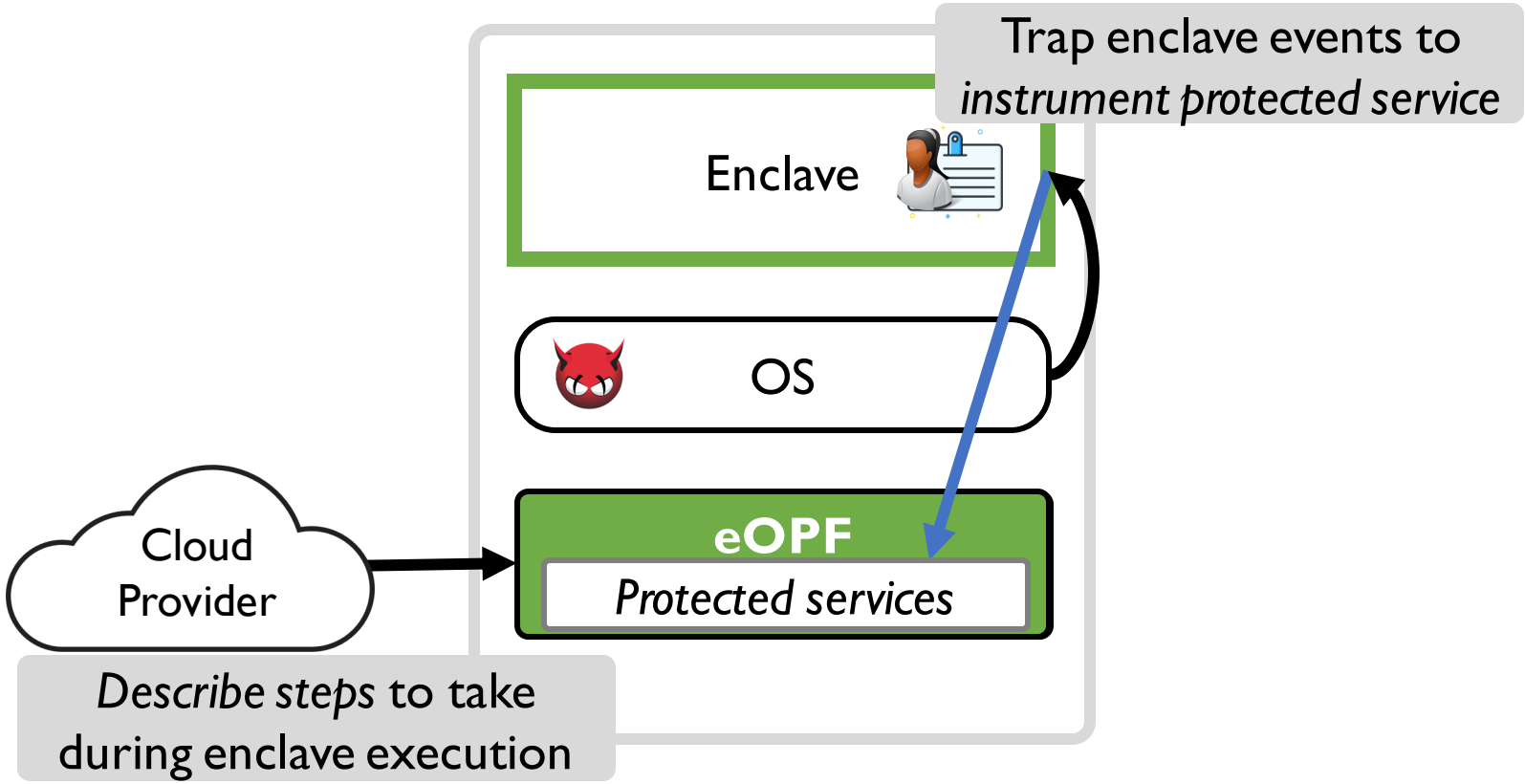


No secure orchestration:
providers rely on untrusted OS

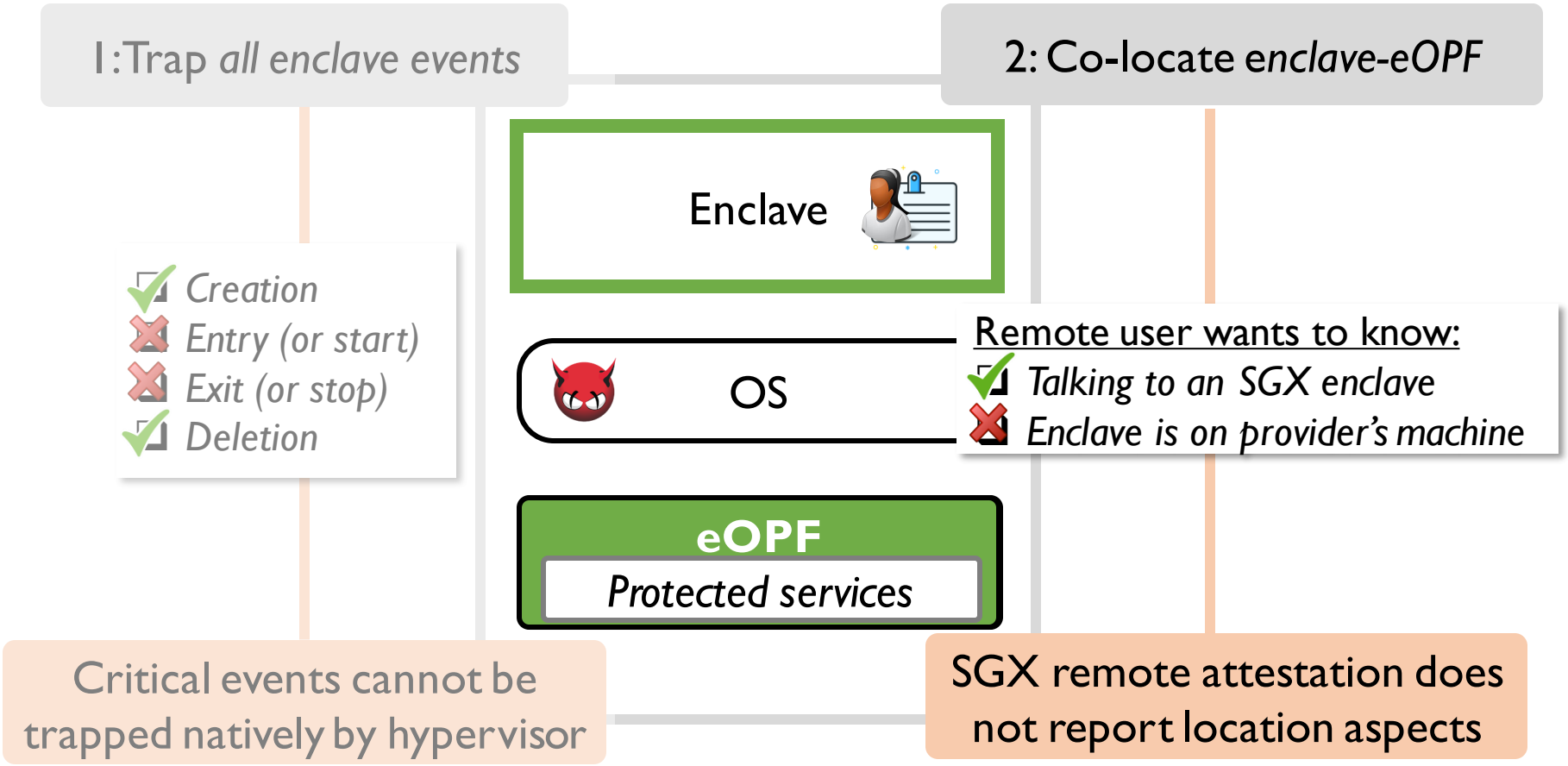
No side-channel defense
against the OS

Standard SGX protection
against hypervisor remain

eOPF augments SGX features using a hypervisor

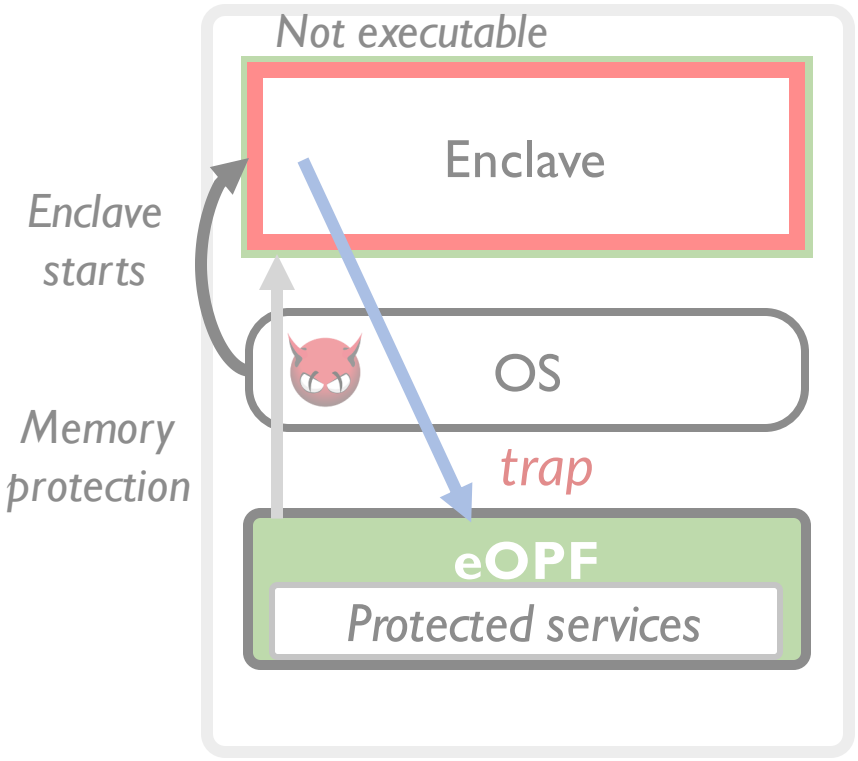


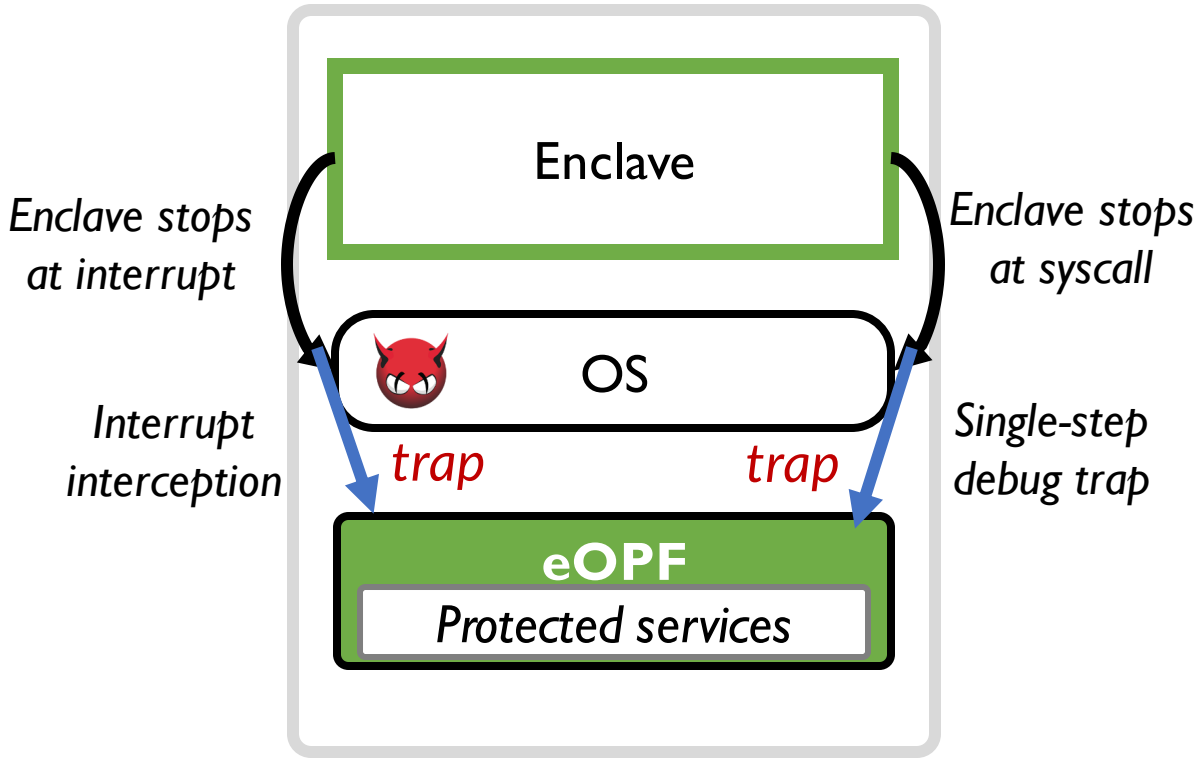
eOPF has two *requirements* for hypervisor instrumentation



How to trap critical events?

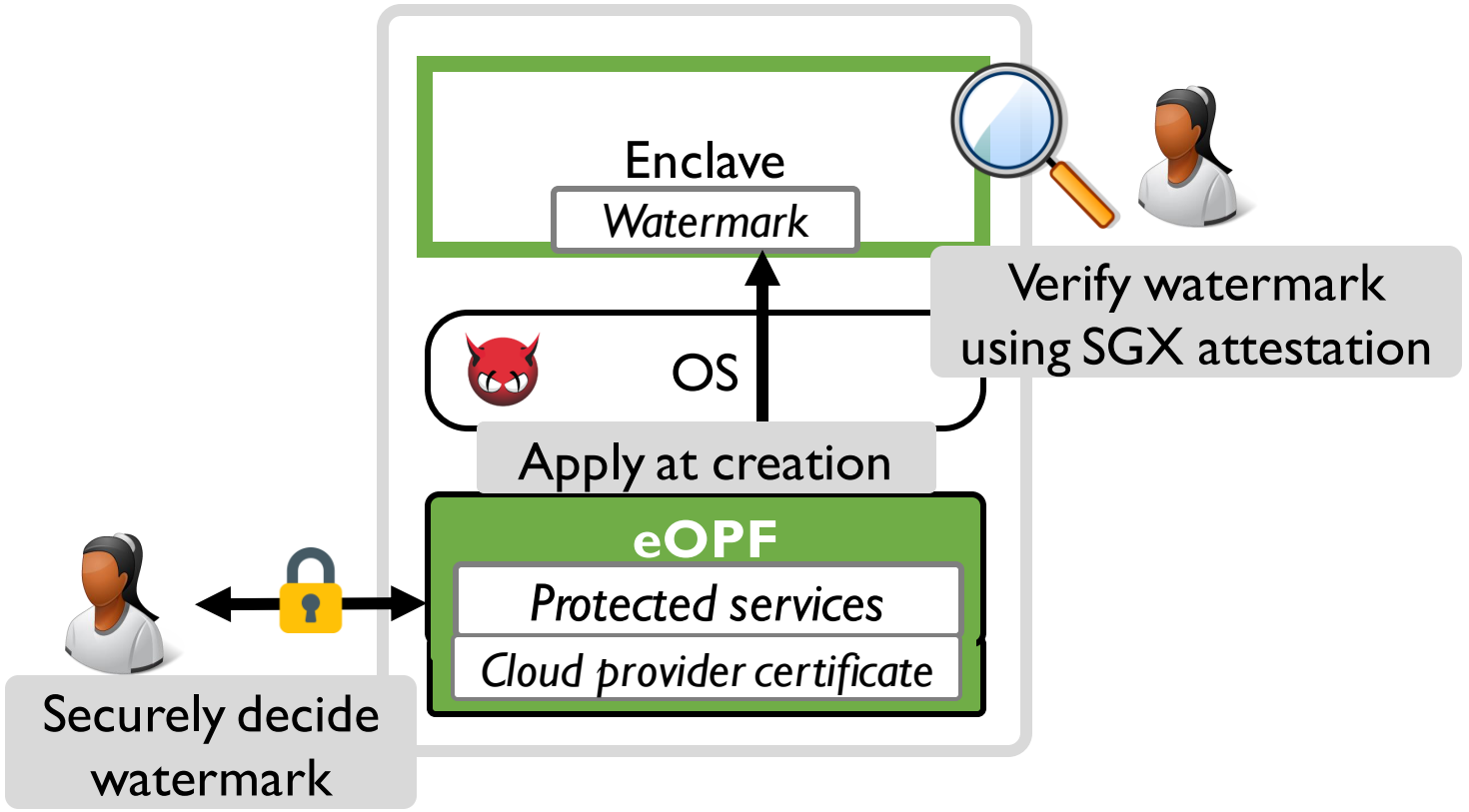
Hypervisors have several features to introspect general software execution



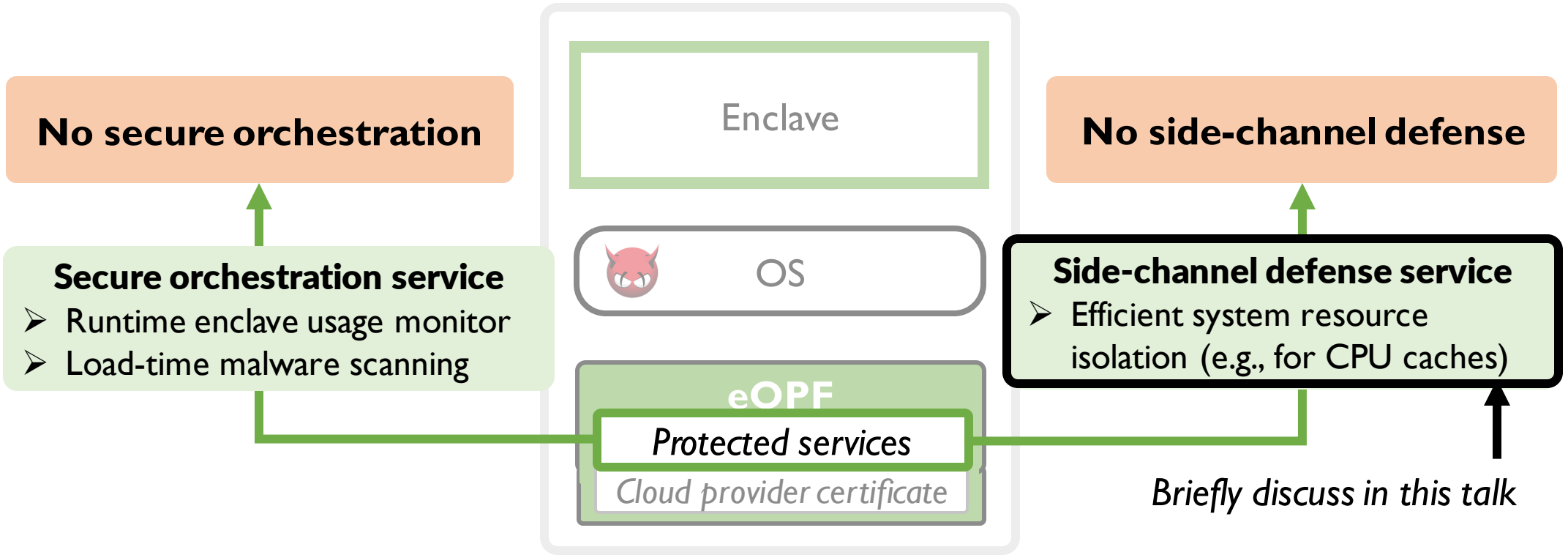


How to attest co-location?

Hypervisors can mark *co-located enclaves* for *verification with SGX attestation*

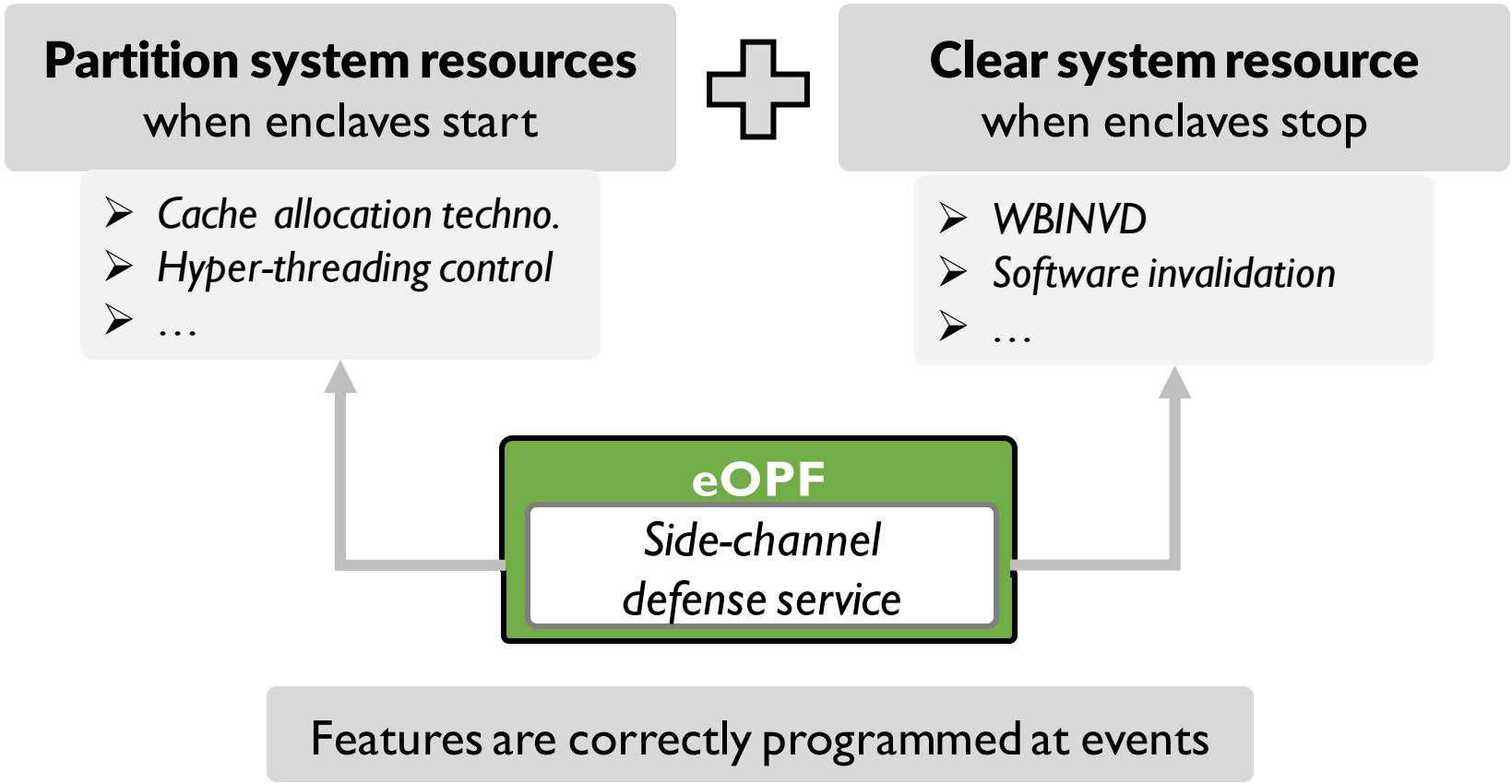


eOPF enables *two features* using implemented services



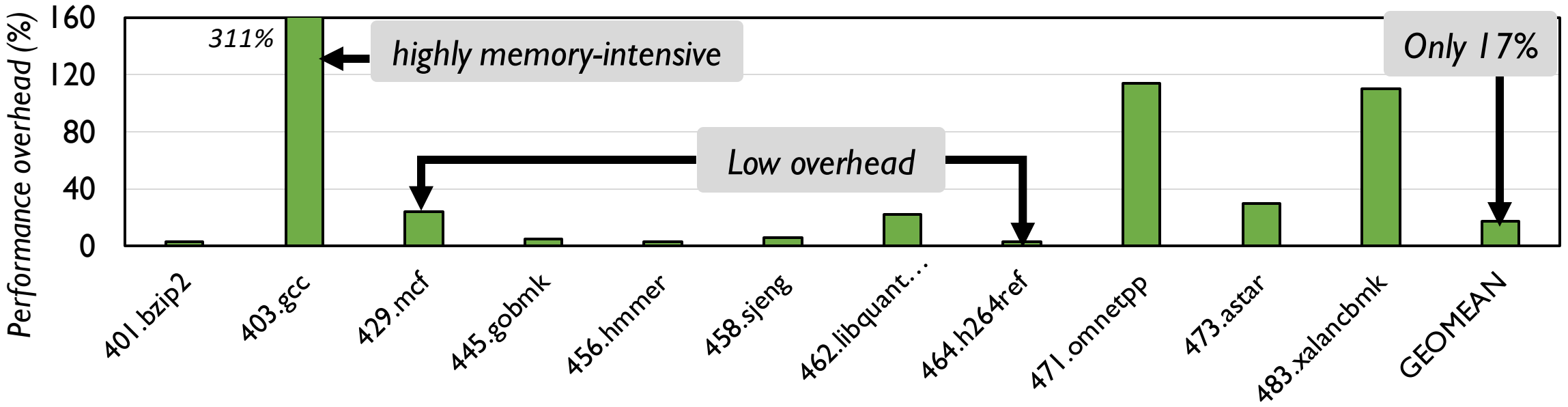
Defending against side-channels with eOPF

- Side-channels arise due to the *sharing* of resources (e.g., CPU caches)



eOPF enables new features with *high performance*

- Ran real-world programs with *secure orchestration* and *side-channel defense* enabled



- Transparently enables strong side-channel defense with a small runtime cost

Key takeaway from *this talk!*