Black Alps 2022

The long and winding road towards secure Confidential Cloud Computing

Elena Reshetova, Intel

Who am I

- Part of Intel SPM Red Team
- Been in security industry for 13 years
- Started in mobile & embedded platform security
- Linux security projects
  - Mostly low-level, i.e. Linux kernel
- Cryptography

Confidential computing

Challenge

Enterprises protect data on storage and in-transit (network)

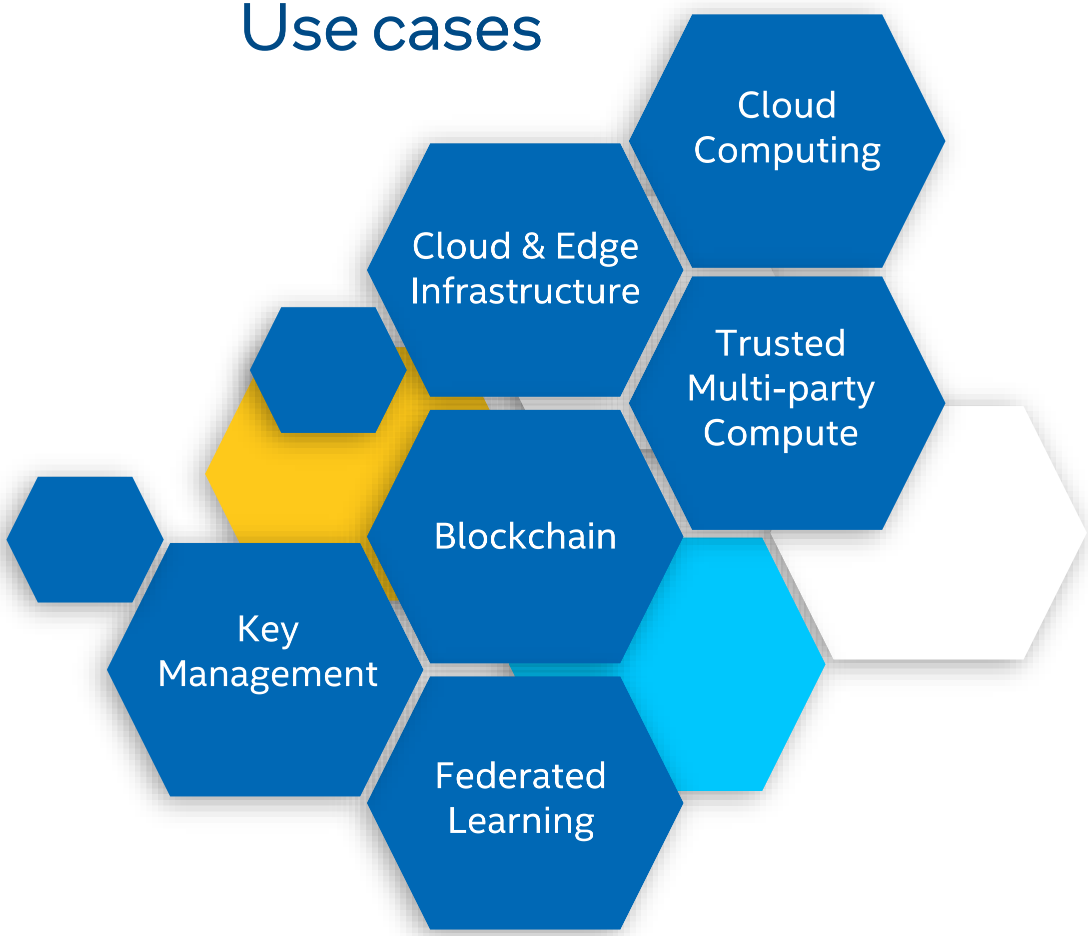
Data confidentiality and integrity in-use (in-memory) is not protected

Solution

Execute the data processing workload in a HW-based Trusted Execution Environment (TEE)

- Requires integrity for the code running inside TEE

Use cases



Confidential Computing Space

CONFIDENTIAL COMPUTING CONSORTIUM

The CC market is poised for exponential growth *

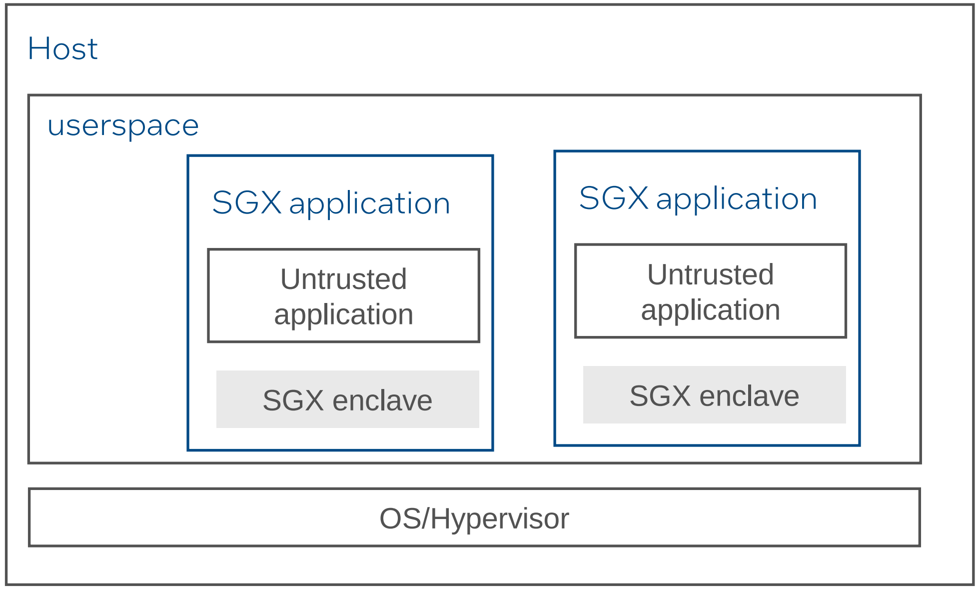
- The Total Addressable Market (TAM) for confidential computing in 2021 is **US$ 1.9-2.0 billion**
- The CC market is expected to grow at a **CAGR of 90-95%** in the best-case scenario and **40-45%** in the worst-case scenario through 2026
- Cyber risks, regulations, and avenues for incremental revenue position CC for hyper growth

* Data from "Confidential Computing – The Next Frontier in Data Security" report, 2021

accenture, ANT GROUP, arm, Google, HUAWEI, intel, Meta, Microsoft, Red Hat, alauda.cn, AMD, AMPERE, anjuna, Baidu, ByteDance, CanaryBit, cisco, CRUST, CYSEC, decentriq, EDGELESS SYSTEMS, ENVEIL, Ethernity CLOUD, Fortanix, HUB, iExec, MARVELL, MITHRIL SECURITY, NVIDIA, Opaque, PHALA NETWORK, Profian, r3., Rivos, RUBY, swisscom, TII Technology Innovation Institute, ULTRAVIOLET, vmware, Western Digital

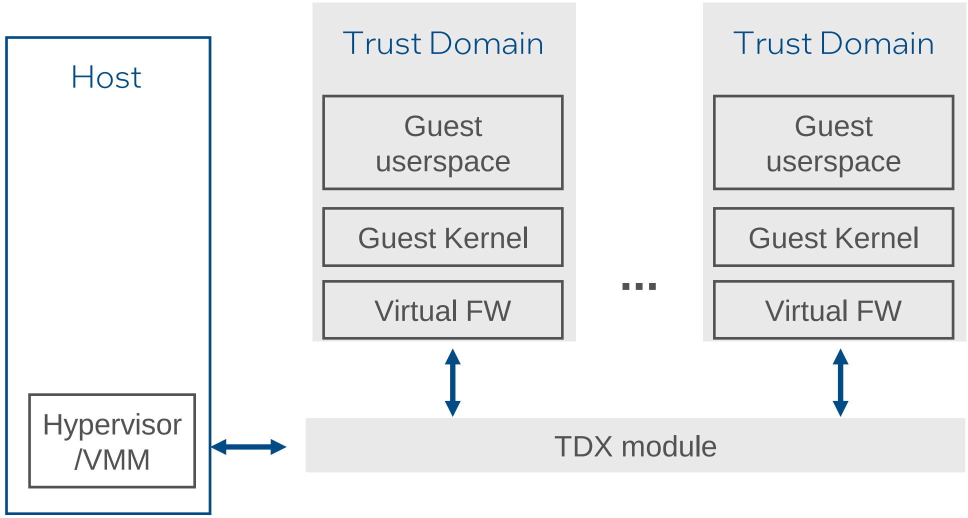
Intel's Confidential Computing solutions

Intel® Software Guard Extensions (SGX)



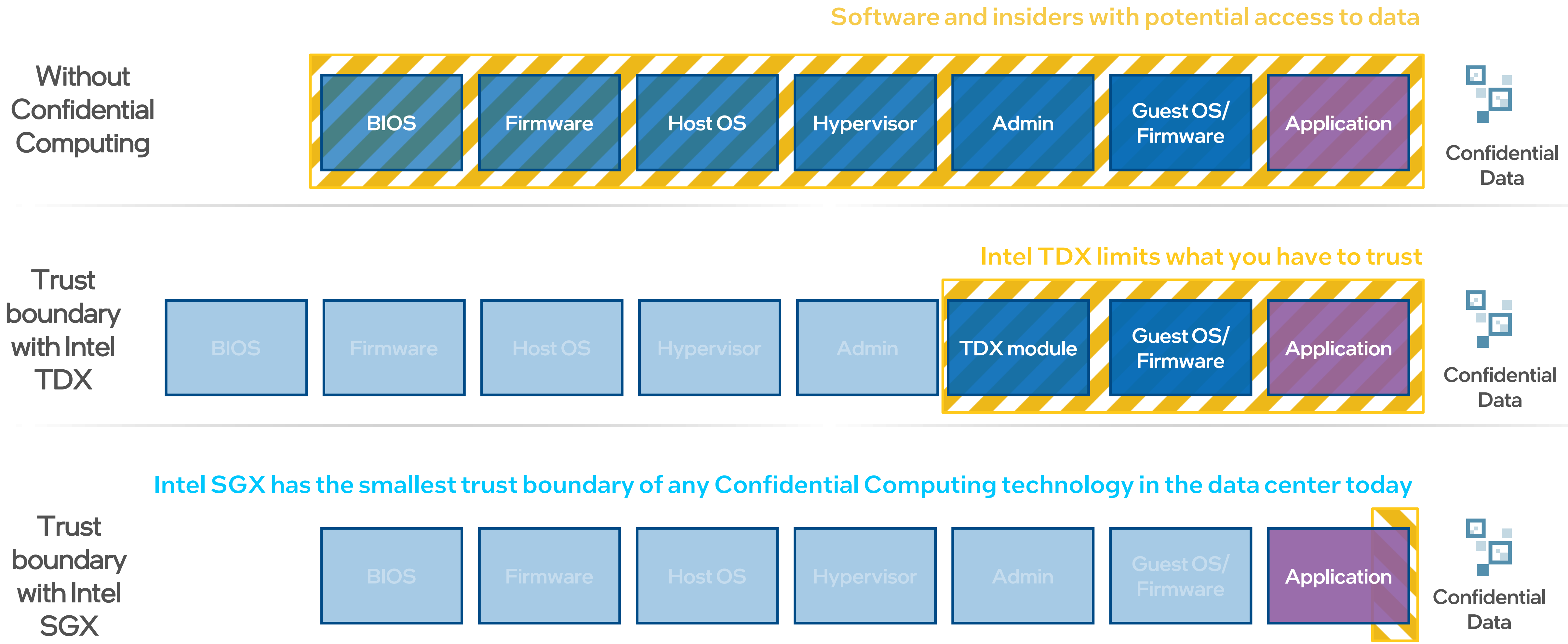
Usages: **Small Trusted Computing Base (TCB) services:** Secure Key Management, Trusted multi-party computation, ...

Intel® Trust Domain Extensions (TDX)



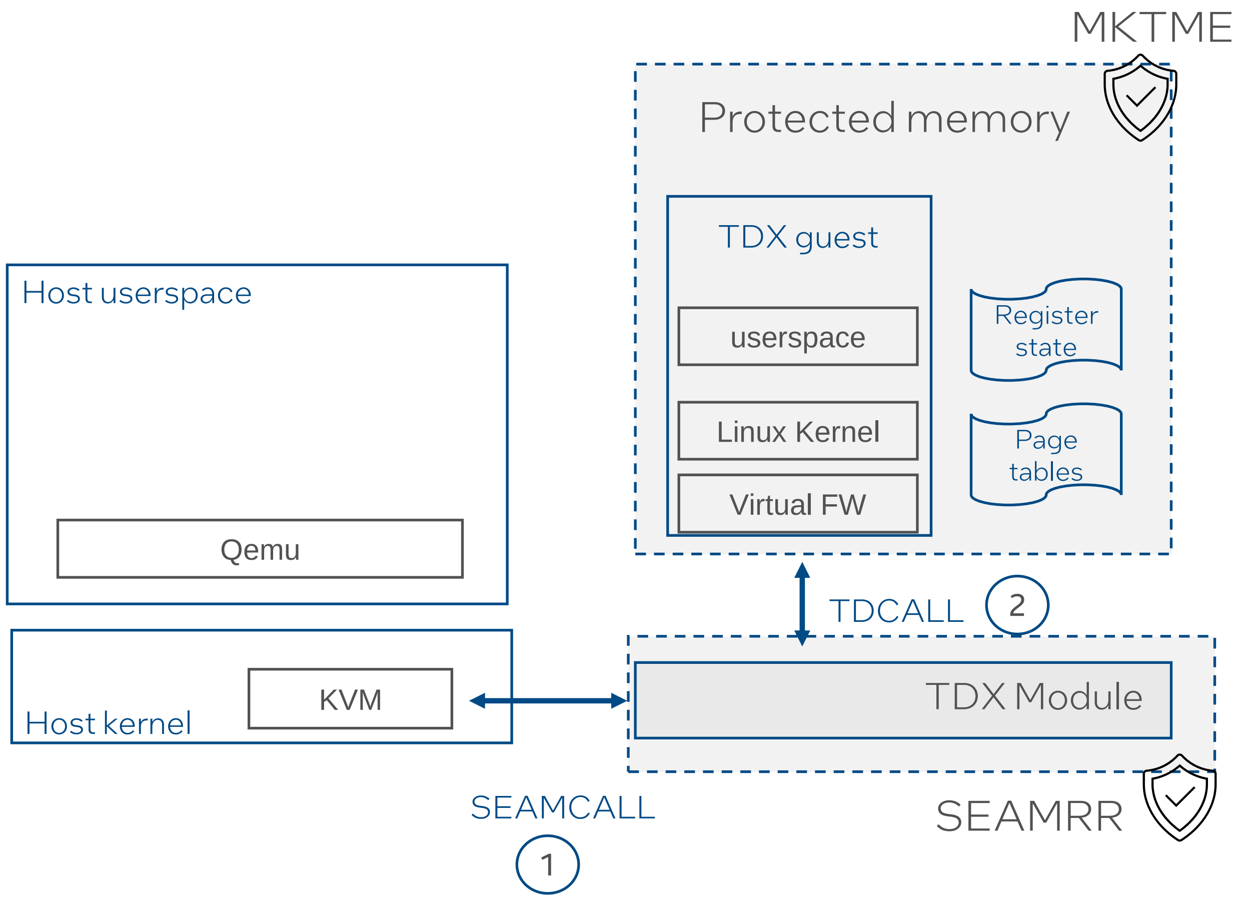
Confidential Cloud Computing, ..

Reduced TCB for CC solutions



Linux Stack for Intel® TDX

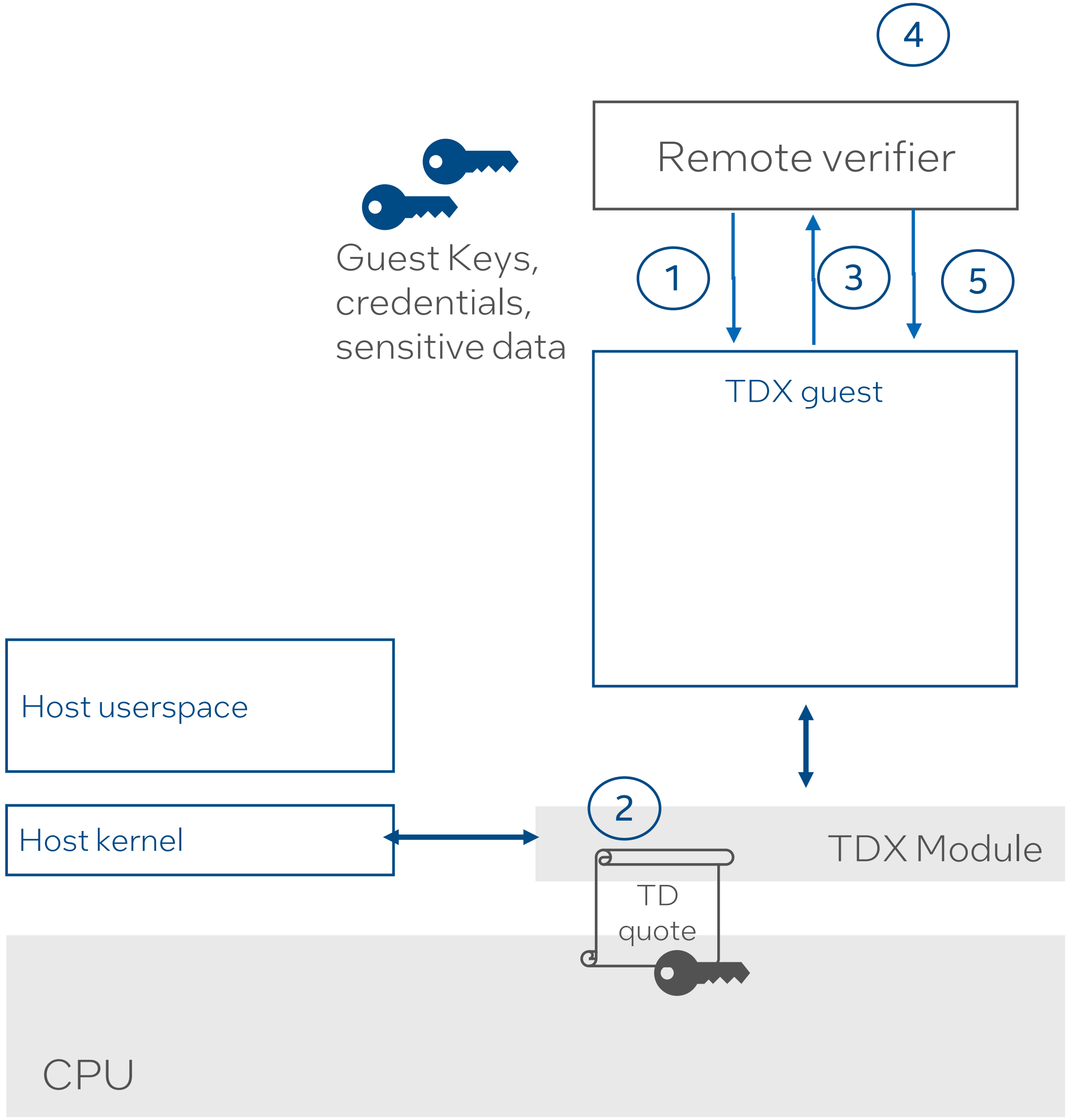
- Components:
  - Hypervisor/VMM: KVM/Qemu
  - Virtual FW: edk2
  - Guest Kernel: TDX-enlighten Linux kernel
- Secure-Arbitration Mode (SEAM) CPU mode
- TDX guest memory protection
  - Multi-Key Total Memory Encryption (MKTME)
- Interfaces: (1) and (2)



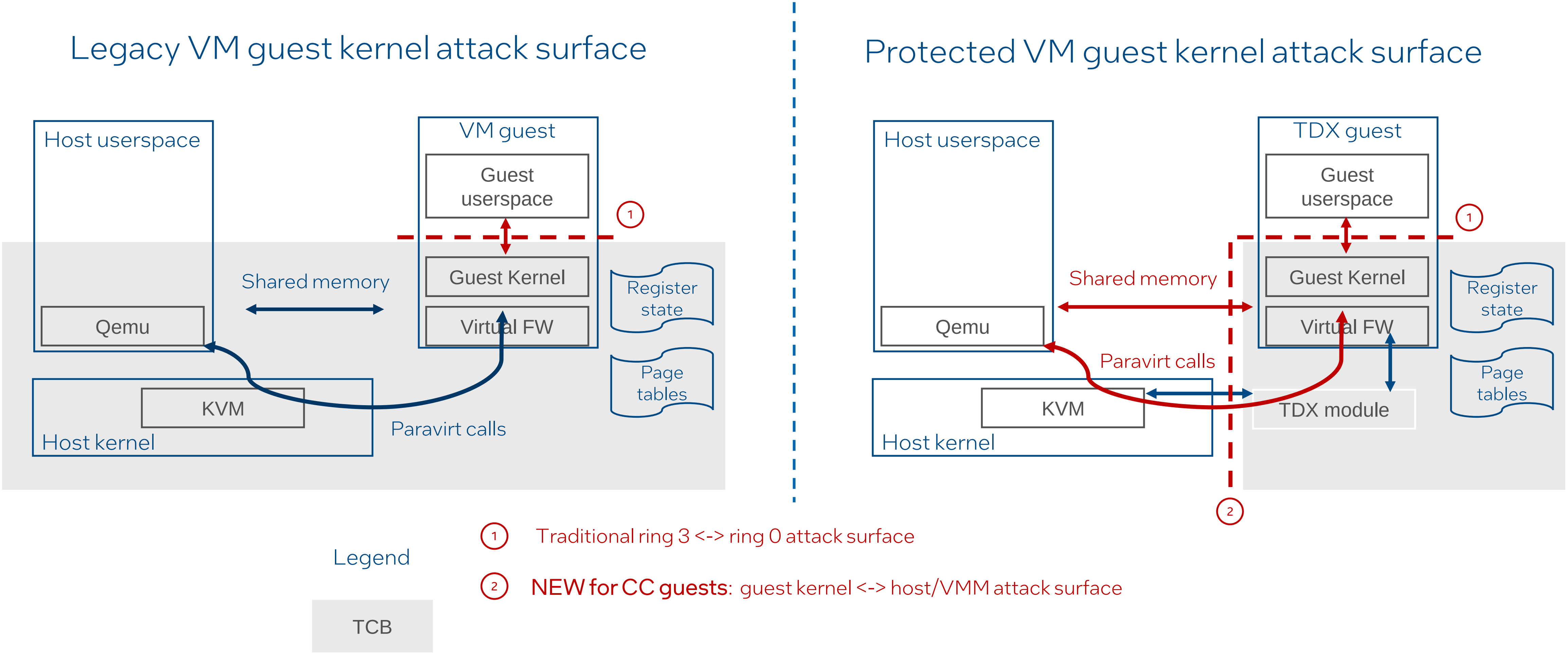
Challenges for Confidential Cloud Computing & Solutions

Deployment & Attestation

- Cloud Service Providers (CSPs) typically provide low-level SW to VM guests
  - This makes them part of TDX guest TCB
- Before releasing secrets into a TDX guest, tenants need to perform attestation
  - Tenants might not be prepared to run attestation service themselves
  - Intel's Project Amber facilitates running CC attestation



Guest SW stack hardening: Guest kernel case



Types of issues

Memory safety

ACPI and AML code security

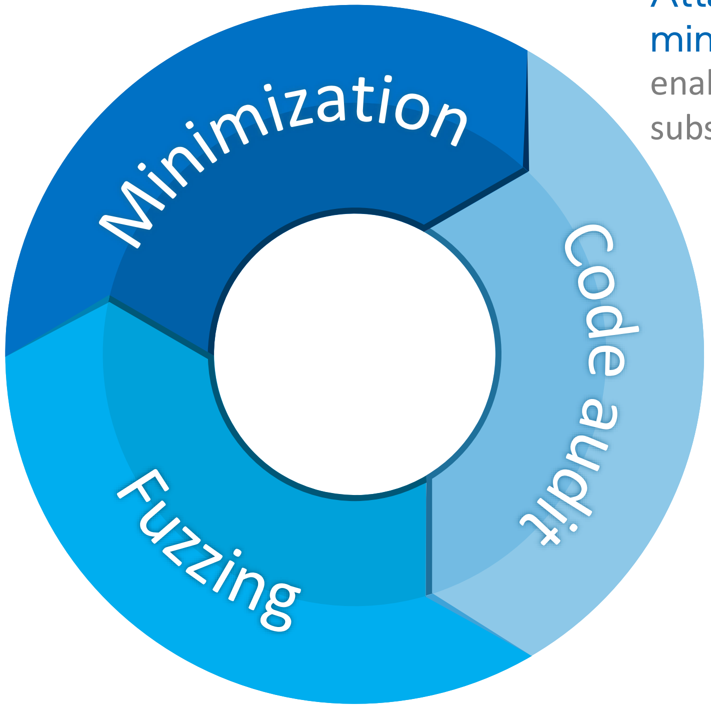
Secure Randomness

Secure Time

Missing IPIs & reliable panic

Transient Execution attacks

TDX Guest Hardening strategy



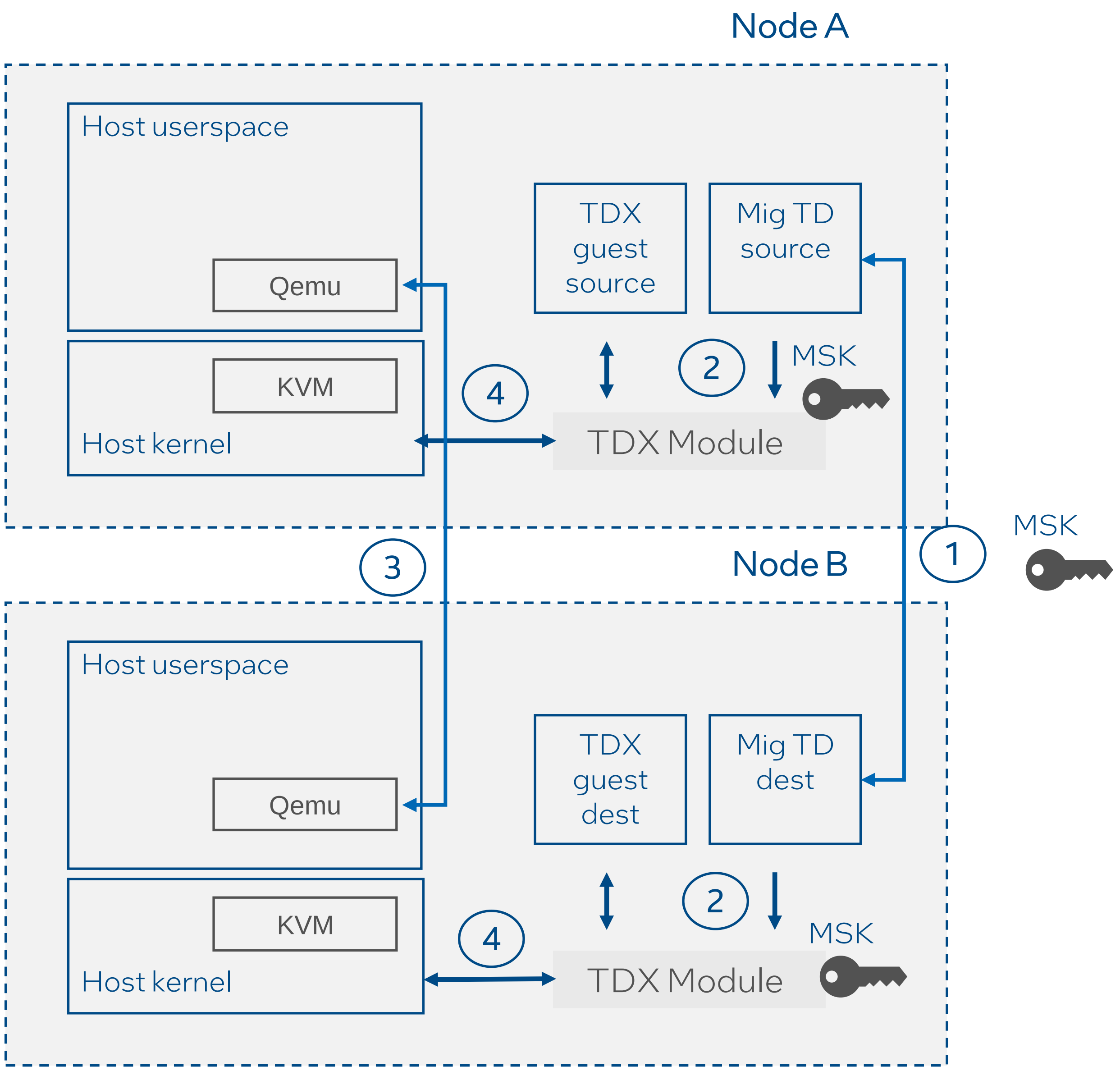
Attack surface minimization: enabled drivers, kernel subsystems, open I/O ports…

Wide scale and targeted fuzzing to exercise the exposed attack surface either in-breath or in-depth for more complex code locations

Static analyzer driven manual code audit to identify problematic places that might need to be disabled, target fuzzed or a code fix might be required

Secure Live Migration

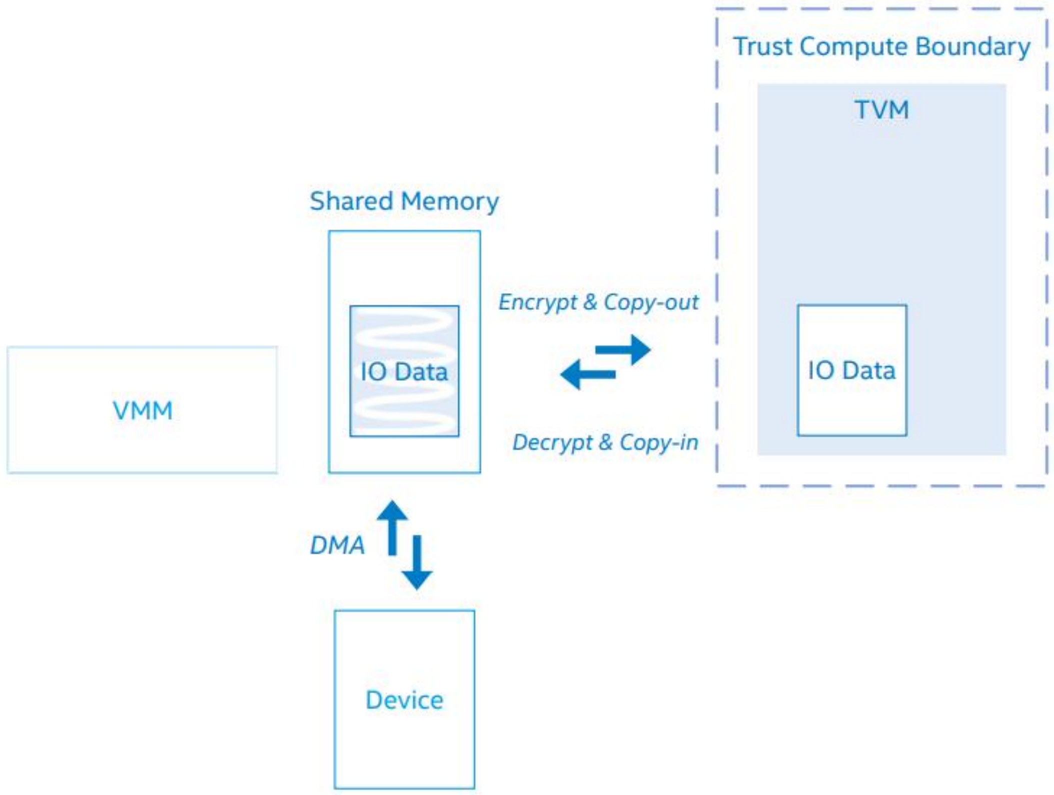
- **Goal**: migrate a TDX guest between different physical nodes
- **Main requirements**:
  - Preserve confidentiality & integrity of TDX guest
  - Fresh TDX guest state
  - No TDX guest cloning
  - Policy-based decision on minimal destination TCB level



Protected guests IO: general case

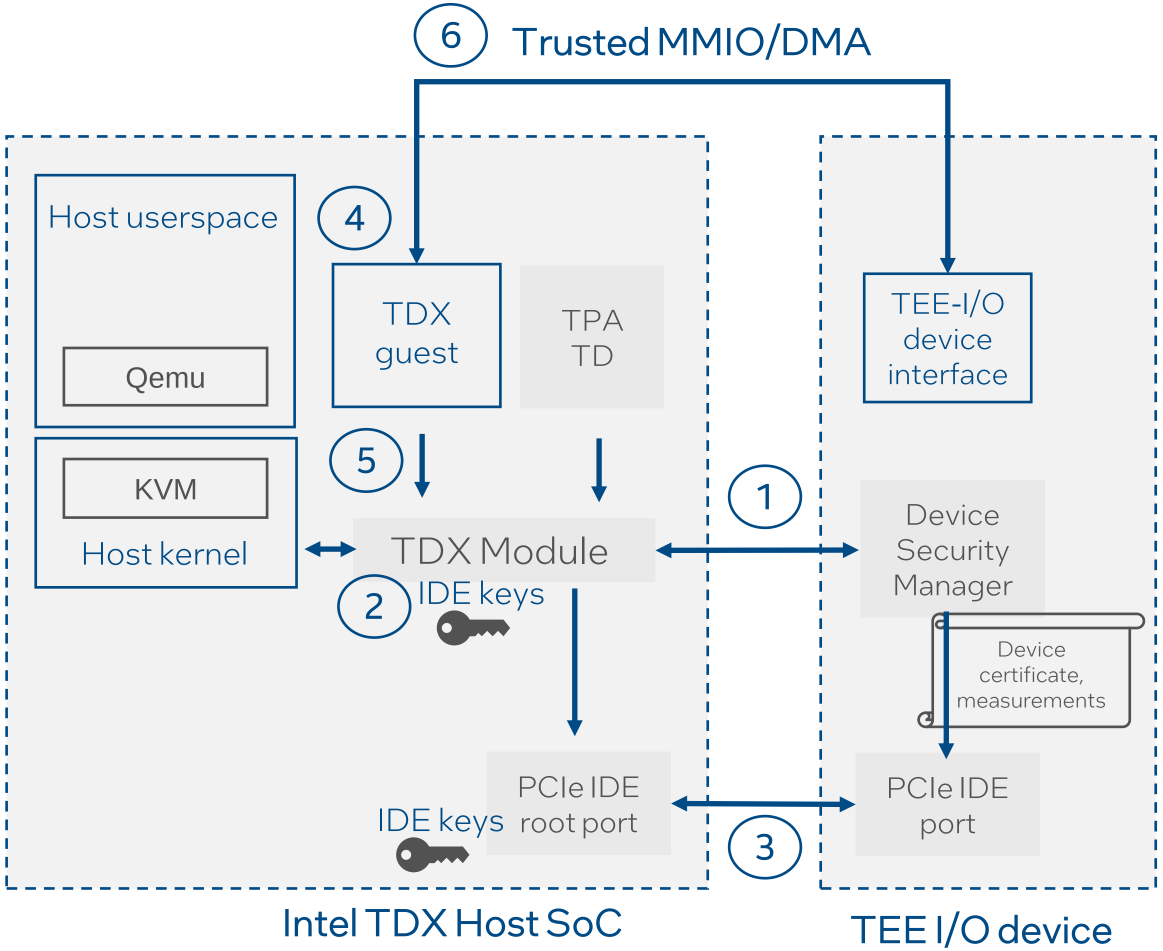
- Physical devices and accelerators are not in TCB of a TDX guest
  - No access to TDX guest private memory

- Set of synthetic devices is used instead, i.e. virtio devices
  - data is staged in shared memory
  - data must be confidentiality & integrity protected
  - performance overhead and robustness



Protected guests IO: Trusted IO

- **Goal**: end-to-end trusted IO between a TDX guest and a TEE-I/O device interface
- **Main requirements**:
  - Policy-based decision on TEE I/O device state and measurements
  - Confidentiality, integrity and replay protection on PCIe link



Conclusions & Takeaways

Moving Towards Secure Confidential Cloud Computing

While technical solutions exist for all known security requirements & use cases

Time for deployment/adoption is required

Intel is committed to drive the best in industry security for CC

References

- Intel® Software Guard Extensions (SGX)
  - https://www.intel.com/content/www/us/en/developer/tools/software-guard-extensions/overview.html
- Intel® Trust Domain Extensions (Intel® TDX)
  - https://www.intel.com/content/www/us/en/developer/articles/technical/intel-trust-domain-extensions.html
- Intel® TDX guest hardening documentation
  - https://intel.github.io/ccc-linux-guest-hardening-docs/index.html
- Project Amber
  - https://www.intel.com/content/www/us/en/security/project-amber.html
- Linux Stack for Intel® TDX
  - https://github.com/intel/tdx-tools

Notices & Disclaimers

Intel technologies may require enabled hardware, software or service activation.

No product or component can be absolutely secure.

Your costs and results may vary.

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document subject to open source software code (OSS) included in this document is licensed under the applicable OSS license from each respective licensor at:

https://github.com/intel/tdx-tools or https://intel.github.io/ccc-linux-guest-hardening-docs/index.html