Linux Kernel Attestation ABI

Context

Kernel attestation ABI

- A userspace Linux kernel interface for generating attestation reports
- Accessible from Linux TVM guests
- Relevant for Intel TDX, AMD SEV, ARM CCA, RISC-V CoVE

Use Cases

- Confidential containers encrypted images
- VM encrypted disk images
- Attested TLS
- …

Problem

One attestation ABI per architecture

- `/dev/sev-guest, /dev/tdx-guest, /dev/arm-cca /dev/cove-guest`, etc
- ioctl based
- Diverging set of commands and replies (one per architecture…)
- Userspace must know its underlying TSM/Architecture

Solution

A `config-fs` ABI

- Userspace sees one single interface across all architectures

Architecture agnostic

- Each architecture is a TSM provider
- Implements and registers a tsm_ops structure

Better scalability than `sysfs`

- One reporting instance per container for example

Solution

A `config-fs` ABI

- Userspace sees one single interface across all architectures

Architecture agnostic

- Each architecture is a TSM provider
- Implements and registers a tsm_ops structure

Better scalability than `sysfs`

- One reporting instance per container for example

```
report=/sys/kernel/config/tsm/report/report0
mkdir $report
dd if=binary userdata plus_nonce > $report/inblob
hexdump $report/outblob
```

Next Steps

- Device attestation reports
  - Devices bound to TSMs
- Runtime measurement register
  - TSM as a root of trust for IMA