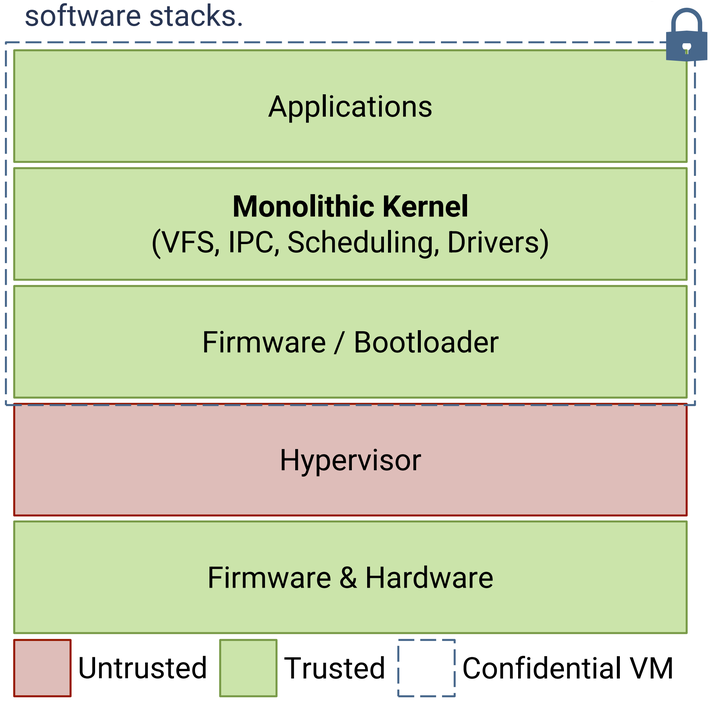
Updates on Confidential Computing with seL4

Alexander Weidinger, Fraunhofer AISEC

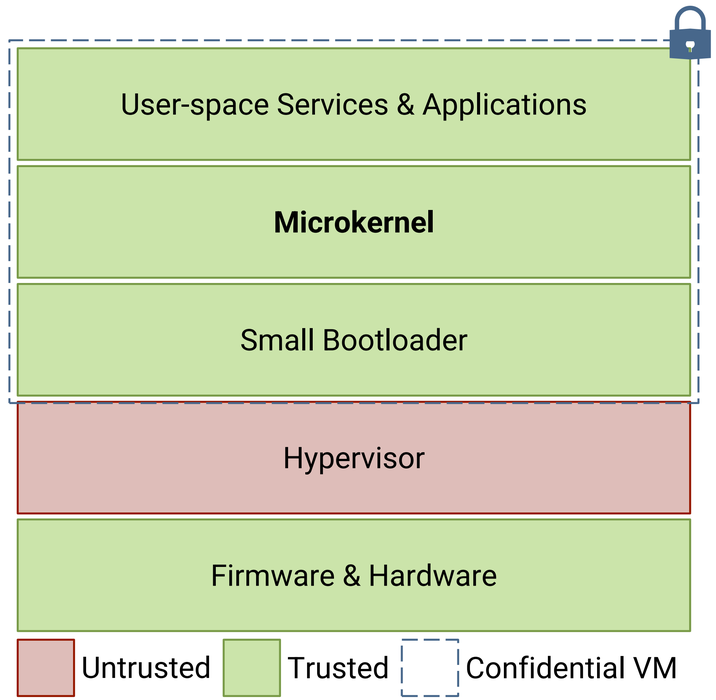
Motivation

- Sensitive data runs in the cloud on infrastructure **we don't control** – it must stay private even from the provider/hypervisor.
- **Data-at-rest** protection is already solved via block encryption (e.g., Full Disk Encryption).
- **Data-in-transit** protection is already solved via transport encryption (e.g., TLS).
- **Data-in-use** protection is still an open problem, which solutions like Intel TDX, AMD SEV-SNP or Arm CCA try to solve.
- Confidential VMs still run a large, highly-privileged guest stack.
- Common software stacks often include OVMF/EDK II, Grub2 and Linux.
- Current advances in the area of agentic AI make it easier to find vulnerabilities in such complex software stacks.



Our Approach

- Replace the guest kernel in the usual software stack with the formally verified seL4 microkernel
- The seL4 microkernel is a particularly slim OS kernel, where only fundamental functionality is executed in kernel-space.
- This provides us with a much reduced TCB and therefore smaller attack surface.



Key Takeaway
Running the formally verified seL4 microkernel as the guest OS shrinks the trusted code inside a confidential VM — smaller attack surface, stronger protection for data in use.

Current State

- We adapted the seL4 microkernel such that it can be executed in a SEV-SNP protected VM.
- We replaced the OVMF / EDK II and Grub2 software stack in our system with an adapted version of qboot, a bootloader with a much smaller TCB.
- We designed an architecture for in-guest attestation of our system.

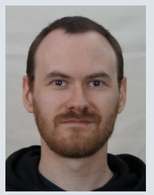
Use Cases

- Secure Block Device
- VPN Gateway
- Secure Key Storage
- Cloud TPM

Next Steps

- Finalize attestation framework.
- Implement sample use case.

I am at the summit! If I am not in front on my poster come and find me to talk about my work.



Alexander Weidinger
Fraunhofer AISEC