Better Security for GPU Drivers

CAPcelerate and Chrompartments

Paul Metzger, Theo Markettos, Matthew Naylor, Timothy Jones
pffm2@cam.ac.uk

Third-party GPU kernel modules are attractive targets for supply chain attacks because they run with kernel privileges.

Software Supply Chain Attacks

- Some software supply chain attacks modify software before it is delivered.
- Among others, this can happen through compromised build systems or compromised developer credentials.
- For example, an attacker could add a backdoor to GPU drivers to attack organisations that use graphics applications or GPGPU computing.

Third-Party GPU Kernel Modules

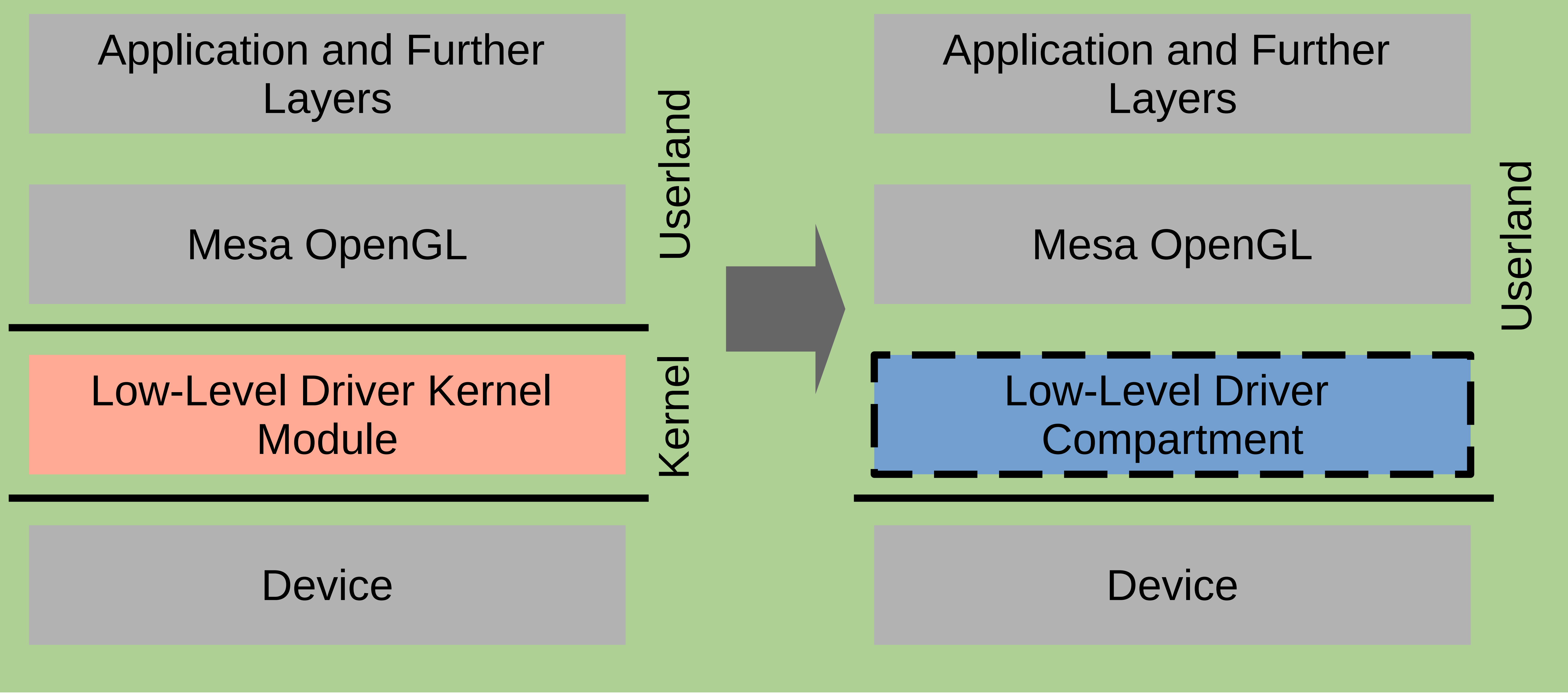
- GPU drivers have a component that runs in the kernel.
- Some vendors provide these as separate closed-source kernel modules that are not part of the kernel source, and so cannot be examined by others.

Solution: Run Third-Party GPU Drivers Purely in User-Space

We de-privilege GPU driver code that is currently shipped in kernel modules by moving it into CHERI compartments in user space.

Current FreeBSD Software Stack

Our Planned Prototype Software Stack


Application and Further Layers
Mesa OpenGL
Low-Level Driver Kernel Module
Device
Userland
Kernel
Application and Further Layers
Mesa OpenGL
Low-Level Driver Compartment
Device
Userland

Low-level GPU drivers will be protected from tampering by other software components in the same address space through CHERI compartments.

We also mitigate kernel data leaks.

DMA

GPU drivers provided by vendors must not have direct control over GPU page tables. Otherwise, a malicious driver could access memory arbitrarily through the GPU by controlling the mapping of virtual GPU addresses to physical addresses. We will investigate the design of a generic kernel service for GPU mappings that sanitises requests made by GPU drivers.

UK Research and Innovation
Digital Security by Design
DSbD.tech
UNIVERSITY OF CAMBRIDGE