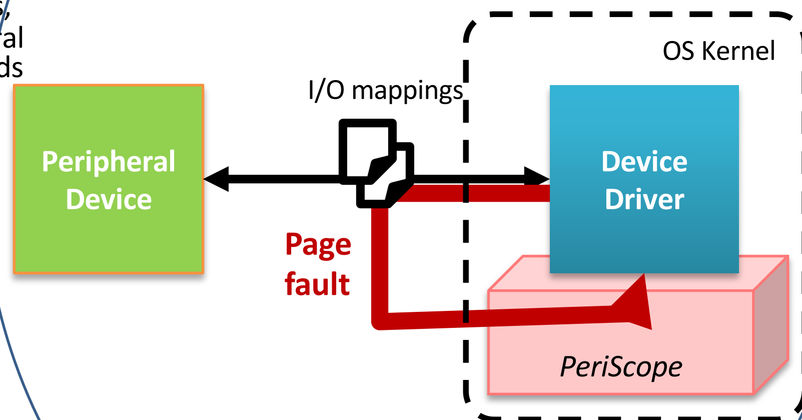
Hydra: Hybrid Defenses for Resilient Applications – Practical Defenses Toward Defense In Depth

Challenge:

- In the traditional security model, application software running “above” the OS is constrained but software running “below” this boundary is often implicitly trusted.
- But in modern connected devices, a malicious input from a peripheral device may trigger a bug that leads to a total system compromise. Demonstrated in real world.

Solution:

- Harden the boundary between the hardware and the OS, to prevent attacks “from below.”
- Use in-Kernel, page-fault based monitoring to explore the hardware/OS boundary. Approach is not device-specific and doesn’t use virtual devices.



Scientific Impact:

- We have created a new technique for finding bugs at the hardware/software boundary and created sharable infrastructure that practices this technique.
- We have released the infrastructure as open source software already, but are working on improving it further.

Broader Impact:

- Our infrastructure has been able to find previously unknown vulnerabilities in the device drivers of flagship phones (Google Pixel and Samsung Galaxy) using both Qualcomm and Broadcomm chips. We were awarded eight distinct CVEs.
- Besides academic publications, we presented at the Qualcomm Security Summit 2019 and at Black Hat 2019.
- Our responsible disclosure resulted in real vulnerabilities being fixed, making the world a safer place.

NSF1619211
University of California, Irvine
Michael Franz, PI – franz@uci.edu