## IRQDebloat：

提出了IRQDebloat原型系统，一种在本身对于系统的外部输入都是通过中断请求发送的这一理解之上，通过自动固件重写来禁用不需要的硬件特性的系统。提出差分trace分析方法。在两种CPU架构、四种操作系统和7种不同的嵌入式SoC平台上测试他们的系统，并发现它能够成功枚举和识别所有注册过的中断处理程序。在Steam Link上，他们调查了攻击面并发现禁用选定的外设可以阻止在过去五年中Linux内核中发现的多达44个cve。从嵌入式设备中获取CPU和内存状态快照转发到PANDA，在PANDA中触发中断并fuzz MMIO收集trace，对收集到的trace做差异分析从而遍历已注册IRQ处理程序，对设备二进制文件做patch禁用对应的IRQ handler，重新烧录回设备并看是否已禁用不必要的处理程序。