研究提出基于软硬件结合的数据流分析芯片加速方案

作者：writer 来源：中国科学院

本文原地址：https://www.iikx.com/news/progress/38051.html

研究提出基于软硬件结合的数据流分析芯片
加速方案
。近日，中国科学院软件研究所团队提出了基于软硬件结合设计的高性能多标签数据流分析方案，为解决实际应用的数据流分析性能瓶颈提供了新思路。

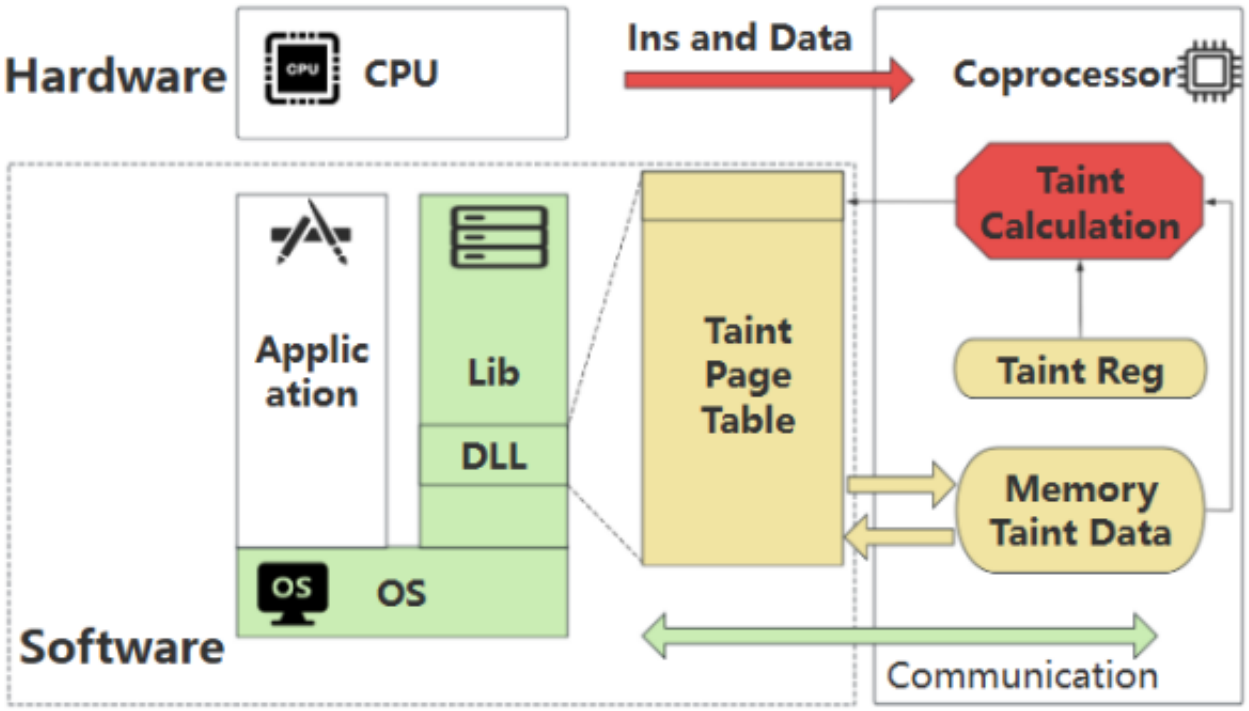
数据流分析是软件分析的基础性方法之一，广泛用于软件安全性分析、漏洞挖掘等研究。当前主流的数据流分析方案多为单标签分析，仅能判断数据是否来源于被标记的数据源，而无法区分数据具体来源的字节位置。在需要细粒度追踪的场景中，必须明确程序中每个受影响字节的具体来源，因而需要多标签分析能力。但是，实现多标签分析需重新设计标签的记录、管理与计算机制，其复杂度高于单标签方案，且缺乏能适用于大规模软件系统的解决方案。

针对上述问题，研究团队提出了软硬件系统结合的多标签分析方案MulcoTaint。该方案基于CPU流水线和协处理器架构，将程序执行逻辑和数据流分析逻辑分离，并通过将数据流标签计算向量化，利用专用协处理器进行硬件加速。同时，团队在软件层面设计了配套机制，使其能够支持二进制/源码的字节级多标签数据流分析。

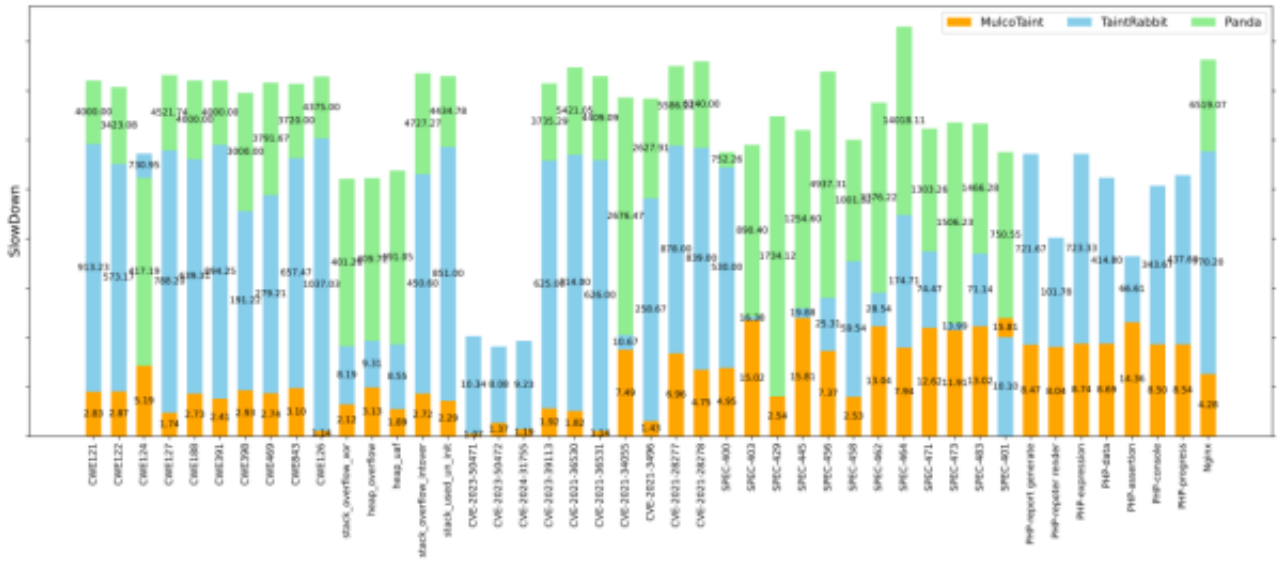
研究团队面向RISC-V指令集，基于开源RISC-V处理器与SoC生成框架Rocket Chip，在现场可编程门阵列（FPGA）上完成MulcoTaint方案并进行了实验验证。结果显示，MulcoTaint的平均性能开销仅为TaintRabbit工具的1/136，是PANDA系统平均性能开销的1/1117，显著提升了数据流分析能力和效率。

未来，MulcoTaint方案有望被引入到处理器架构设计中，为新型程序分析能力和安全机制设计提供基础性支撑。

相关论文被网络安全领域顶级会议USENIX Security
2026录用。研究工作得到国家自然科学基金等的支持。



MulcoTaint分析系统架构



MulcoTaint分析性能效果

研究团队单位：软件研究所