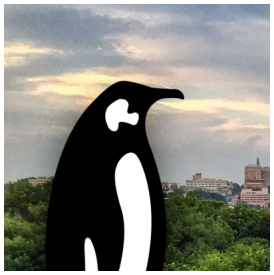

Contribution ID: **287** Type: **not specified**

Advancing Kernel Control Flow Integrity with eBPF

Monday, 13 November 2023 17:00 (30 minutes)

We explore the use of eBPF for kernel security, specifically in the context of enforcing kernel control flow integrity (kCFI). CFI is an effective way to defend against control hijack attacks. However, current CFI implementation in the kernel is imprecise and suffers from deployment challenges, resulting in it being underused. We believe eBPF's intrinsic strengths (safety, access to runtime state, dynamicity) can address both the imprecision and deployment issues of kCFI. In this talk, we will discuss the challenges of using eBPF to enforce fine-grained and precise kCFI. We will also discuss techniques to reduce the eBPF invocation cost while maintaining the flexibility of eBPF, a key challenge of this approach. We will present the detailed workings of our eBPF-based kCFI implementation and the evaluation of its performance overhead.

From this talk, audiences will understand the current limitations of kernel CFI, opportunities/challenges of using eBPF for kCFI, and approaches to overcome those challenges. This discussion will help highlight issues and ways of using eBPF not only for kCFI, but overall kernel security and spur further discussion about the feasibility of such an approach.

Primary authors: JIA, Jinghao (UIUC); LE, Michael (IBM); AHMED, Salman (IBM); WILLIAMS, Dan (Virginia Tech); JAMJOOM, Hani (IBM); XU, Tianyin (University of Illinois at Urbana-Champaign)

Presenter: JIA, Jinghao (UIUC)

Session Classification: eBPF & Networking

Track Classification: eBPF & Networking Track