STEVENS
INSTITUTE OF TECHNOLOGY
1870

Ph.D. DISSERTATION DEFENSE

Candidate:	Konstantinos Kleftogiorgos
Degree:	Doctor of Philosophy
School/Department:	Charles V. Schaefer, Jr. School of Engineering and Science / Computer Science
Date:	July 11, 2025
Time:	10:00 AM EDT
Location:	Virtual (https://stevens.zoom.us/j/91724044286)
Title:	OFFLOADING SECURITY CHECKS VIA SOFTWARE-DRIVEN LOGGING
Chairperson:	Dr. Dave Naumann, Professor and Chair, Department of Computer Science, Charles V. Schaefer, Jr. School of Engineering and Science, Stevens Institute of Technology
Committee Members:	Dr. Georgios Portokalidis, Associate Research Professor, IMDEA Software Institute; Visiting Research Professor, Department of Computer Science, Stevens Institute of Technology Dr. Michael Greenberg, Assistant Professor, Department of Computer Science, Charles V. Schaefer, Jr. School of Engineering and Science, Stevens Institute of Technology Dr. Jun Xu, Assistant Professor, School of Computing, University of Utah

ABSTRACT

Memory-unsafe languages such as C and C++ are foundational to systems programming, but they present a persistent security challenge due to their susceptibility to memory corruption attacks. The prevailing defense strategies present a difficult trade-off. Inline software monitors, while broadly deployable on existing systems, often incur significant performance overhead and introduce architectural weaknesses. In contrast, specialized hardware defenses that offer stronger security guarantees are not yet widely available, limiting their immediate impact. This dissertation explores a third path, investigating how security enforcement can be efficiently and securely offloaded from an application by repurposing features already present in commodity processors. First, we introduce SideCar, a framework that leverages Software-Driven Logging (SDL) capabilities in commodity processors—Intel Processor Trace and Arm CoreSight—to create secure, tamper-resistant channels for offloading security checks to parallel monitors. SideCar demonstrates versatility through three security policies: SideCFI reduces CFI latency by 30% compared to LLVM-CFI, SideStack provides enhanced shadow call stack security, and SideASan enables complex memory error detection. Our monitors require 30× fewer resources than prior approaches, demonstrating the efficiency of SDL-based security offloading. Building on this foundation, we develop StreamCFI, the first SDL-based framework to enforce dynamic CFI policies. By combining type-based and per-input activation policies with optimized logging, StreamCFI reduces attack surface by 80% while achieving 15% performance improvement over state-of-the-art solutions and outperforming LLVM-CFI by 3.8% on real-world applications. Finally, to bring clarity to the diverse and often conflicting ways CFI is measured and to understand the security benefits of dynamic policies, like StreamCFI's, we conduct a systematic analysis of proposed evaluation metrics. This research collectively demonstrates that repurposing existing hardware debugging features enables a new class of low-latency, parallel security monitors. By achieving strong security guarantees without the performance penalties of inline approaches, this work paves the way for the practical deployment of advanced defenses in performance-critical systems.