BINGHAMTON UNIVERSITY
STATE UNIVERSITY OF NEW YORK
Computer Science

THE DEPARTMENT OF COMPUTER SCIENCE & THE COMPUTER SCIENCE GRADUATE STUDENT ORGANIZATION (GSOCS) PRESENT

INVITED SPEAKER SERIES

Dr. Trent Jaeger
Penn State University

Friday, 11/18 at noon, EB-110 (Engineering Building, Main Campus)

Title: Fine-Grained Control-Flow Integrity for Kernel Software

Abstract: Modern systems assume that privileged software always behaves as expected, however, such assumptions may not hold given the prevalence of kernel vulnerabilities. One idea is to employ defenses to restrict how adversaries may exploit such vulnerabilities, such as Control-Flow Integrity (CFI), which restricts execution to a Control-Flow Graph (CFG). However, proposed applications of CFI enforcement to kernel software are too coarse-grained to restrict the adversary effectively and either fail to enforce CFI comprehensively or are very expensive. We present a mostly-automated approach for retrofitting kernel software that leverages features of such software to enable comprehensive, efficient, fine-grained CFI enforcement. We achieve this goal by leveraging two insights. We first leverage the conservative function pointer usage patterns found in the kernel source code to develop a method to compute fine-grained CFGs for kernel software. Second, we identify two opportunities for removing CFI instrumentation relative to prior optimization techniques: reusing existing kernel instrumentation and creating direct transfers, where possible. Using these insights, we show how to choose optimized defenses for kernels to handle system events, enabling comprehensive and efficient CFI enforcement. We evaluate the effectiveness of the proposed fine-grained CFI instrumentation by applying the retrofitting approach comprehensively to FreeBSD, the MINIX microkernel system, and MINIX's user-space servers, and applying this approach partly to the BitVisor hypervisor. We show that our approach eliminates over 70% of the indirect targets relative to the best current, fine-grained CFI techniques, while our optimizations reduce the instrumentation necessary to enforce coarse-grained CFI. The performance improvement due to our optimizations ranges from 51%/25% for MINIX to 12%/17% for FreeBSD for the average/maximum microbenchmark overhead. The evaluation shows that fine-grained CFI instrumentation can be computed for kernel software in practice and can be enforced more efficiently than coarse-grained CFI instrumentation.

Bio: Trent Jaeger is a Professor in the CS and Engineering Department at The Pennsylvania State University and the Co-Director of the Systems and Internet Infrastructure Security (SIIS) Lab. He is a well-known expert in computer systems security having published over 100 peer-reviewed papers on these topics and is the author of the book "Operating Systems Security," which examines the principles of secure operating systems. Dr. Jaeger's research has resulted in several contributions to the security of the Linux kernel, including the Linux Security Modules framework, Linux Integrity Modules framework, and the integration of IPsec with SELinux. His current research focuses on the development of system mechanisms and program analysis techniques to harden deployments in mobile, server, and cloud environments. Dr. Jaeger is currently the Chair of the ACM Special Interest Group on Security, Audit, and Control (ACM SIGSAC), which is the security research community with nearly 1000 members. He has been the program chair of several conferences and workshops, including ACM ASIACCS in 2014. He previously worked at IBM Research from 1996 to 2005, when he joined Penn State.