DISTINGUISHED WEBINAR SERIES IN ARTIFICIAL INTELLIGENCE AND CYBER SECURITY

Verifying the eBPF Verifier in the Linux Kernel

Featuring Dr. Santosh Nagarakatte

Professor and Undergraduate Program Director,

Department of Computer Science,

Rutgers University, New Brunswick.

Abstract:

This talk describes our experience deploying automated verification techniques for proving the correctness of value tracking components of the eBPF verifier in the Linux Kernel over the last four years. The eBPF verifier uses abstract interpretation with multiple abstract domains for value tracking. The Linux kernel uses non-standard approaches for refining the results from multiple abstract domains, which necessitated us to design new techniques to show their correctness. During this process, we also discovered that some of the abstract operators are unsound in isolation. The unsoundness of these operators are eventually corrected by a shared refinement operator. The presence of intermediate "latent" unsound abstract operators makes the task of automated verification harder. Our patches to the Linux kernel, which have been upstreamed, fix these latent errors and make the abstract operators correct in isolation, which enables faster automated verification.

Biography:

Dr. Santosh Nagarakatte is a Professor and Undergraduate Program Director of Computer Science at Rutgers University. He obtained his PhD from the University of Pennsylvania in 2012. His research interests are in Hardware-Software Interfaces spanning Programming Languages, Compilers, Software Engineering, and Computer Architecture. His papers have been selected as IEEE MICRO Top Picks papers of computer architecture conferences in 2010 and 2013. He received the NSF CAREER Award in 2015, ACM SIGPLAN PLDI 2015 Distinguished Paper Award, ACM SIGSOFT ICSE 2016 Distinguished Paper Award, and 2018 Communications of the ACM Research Highlights paper for his research on LLVM compiler verification. His PhD student David Menendez's dissertation on LLVM verification was awarded the 2018 ACM SIGPLAN John C Reynolds Outstanding Dissertation Award. His papers on correctly rounded elementary functions have been recognized with the ACM SIGPLAN PLDI 2021 Distinguished Paper Award and the ACM SIGPLAN POPL 2022 Distinguished Paper Award. His PhD student Jay Lim's dissertation on correctly rounded elementary functions was awarded the 2022 ACM SIGPLAN John C Reynolds Outstanding Dissertation Award. He was selected as an ACM Distinguished Member in 2023.

DATE:
Thursday, June 5th, 2025

TIME:
11:00-11:50 a.m. CST

LOCATION:
Virtual

Webinar LINK:
Join Directly

The **Distinguished Speaker Webinar Series** is aimed to advance the state-of-the-art concepts and methods in artificial intelligence and cyber security areas. The series is jointly hosted by the Center for Cyber Security Research (C2SR), the Artificial Intelligence Research (AIR) Initiative, and the School of Electrical Engineering and Computer Science (SEECS) at the University of North Dakota College of Engineering & Mines with support from University of Minnesota, North Dakota State University, University of Miami, Texas A&M Kingsville, University of Connecticut and West Virginia University.

For inquires please contact UND.C2SR@und.edu