School of Computing
UNIVERSITY OF GEORGIA

Faculty Candidate Seminar

February 18, 2026
11:15 am - 12:30 pm – Room: Boyd 306

Grounding Software Security Agents with Program Analysis

Dr. Penghui Li
Postdoctoral Research Scientist – Columbia University

Abstract:

Large Language Model (LLM)-based agents have shown great promise in automating complex software security tasks such as vulnerability detection and patching. However, most existing agents treat programs as unstructured free text, leading to inefficient context retrieval and hallucinated reasoning about program behavior. This talk presents my research vision for grounding software security agents in program analysis foundations. The central insight is that software programs are not free text and convey program semantics. I will first introduce Neo that grounds agent context in structural semantics to locate vulnerable code. I will then present validation techniques that use execution semantics to eliminate hallucinations and confirm these vulnerabilities. This grounded agentic framework achieves a 3.8× reduction in context retrieval iterations and a 31.6× reduction in token usage. It also identified high-impact vulnerabilities in widely-deployed software such as GitLab and WordPress, safeguarding their millions of users. I will conclude my talk with my future research agenda toward autonomous, generalizable software security.

Biography:

Penghui Li is a Postdoctoral Research Scientist at Columbia University. His research focuses on software system security and its intersection with machine learning. Most recently, he builds infrastructure to ground LLM-based software security agents with stronger guarantees and improved efficiency. Penghui has discovered over 300 security vulnerabilities, leading to patches in foundational systems such as the Linux kernel and GitHub platform. Penghui's work has been recognized with a Distinguished Paper Award, a Best Paper Honorable Mention, and a Distinguished Artifact Award at ACM CCS. He also received two Distinguished Reviewer Awards.

Sponsored by the University of Georgia, School of Computing