NJIT

Department of Computer Science

Advancing Binary Code Analysis: Bridging Foundational Techniques and AI-Driven Innovations

Haotian Zhang
University of Texas at Arlington

Hosted by: Zephyr Yao

Date: Wednesday, February 12, 2025
Coffee: 2:15 PM – 2:30 PM
Time: 2:30 AM – 3:30 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)

Zoom Link: https://njit-edu.zoom.us/j/97177170167?pwd=Gx6HgJLEbJuCzVrbn0qXdVxPce4lby.1

Meeting ID: 971 7717 0167
Passcode: 587047

Abstract:
Binary code analysis is fundamental to securing modern software systems, enabling critical tasks such as vulnerability detection, malware analysis, and program hardening. In this talk, I will present a two-part exploration of my research contributions to this domain. The first part focuses on traditional program analysis techniques, including symbolic execution and precise analysis methods, which are utilized to systematically debloat software and reduce attack surfaces. This includes the development of a framework specifically designed for debloating MIPS shared libraries in firmware. The second part highlights my efforts to integrate advanced machine learning approaches into binary analysis. I will demonstrate how graph neural networks (GNNs) and natural language processing (NLP) models can enhance the resolution of indirect control flows, addressing long-standing challenges in binary code representation and analysis. By synthesizing classical methodologies with cutting-edge AI techniques, my research provides novel solutions to improve the security and reliability of software systems.

Bio:
Dr. Haotian Zhang is a researcher with expertise in software and systems security. He earned his Ph.D. in Computer Engineering from the University of Texas at Arlington. His research focuses on binary code analysis, malware detection, and the application of machine learning techniques to cybersecurity challenges. Dr. Zhang has published his work in premier venues, including ASPLOS, USENIX Security, and CCS, and has received multiple awards, such as recognition in the ACM and PLDI Student Research Competitions. His work bridges foundational program analysis with advanced machine learning methods to tackle pressing issues in software security and reliability.