NJIT

Department of Computer Science

Combating Cyber Attacks by Securing the Software Lifecycle

Yuchen Zhang
New York University

Host: Reza Curtmola

Date: Friday, March 14, 2025
Coffee: 11:15 AM – 11:30 AM
Time: 11:30 AM – 12:30 PM (Eastern Time (US and Canada)
Location: GITC 4402 (4th floor Seminar Lecture Hall)

Zoom Link: https://njit-edu.zoom.us/j/97284314134?pwd=TVQyOUBqMUYiybTnHCJ3SaKryXUr94.1

Abstract:

This talk proposes a holistic strategy for combating cyber threats by addressing security challenges at each stage of the software lifecycle—from adopting memory-safe programming languages to refining post-deployment vulnerability detection and supply chain integrity. It begins by highlighting real-world examples of cyber attacks and the role that memory safety lapses play in enabling exploits. The talk then examines Rust as a case study in safe programming, exploring how runtime checks and “unsafe” code segments can introduce performance overhead or security risks. Building on these insights, the presentation discusses an optimized AddressSanitizer (ASan--) that significantly reduces runtime overhead while preserving robust detection capabilities, aiding in large-scale software testing. Finally, it focuses on enhancing Software Bill of Materials (SBOM) with code coverage techniques (CovSBOM) to cut down on false positives and better prioritize vulnerabilities, thus improving overall supply chain security. By integrating safe language practices, efficient sanitization, and high-fidelity SBOM-based scanning, this talk underscores the importance of an end-to-end security framework for protecting modern software ecosystems.

Bio:

Yuchen is currently a postdoctoral researcher in the Secure Systems Laboratory (SSL) at the Tandon School of Engineering, New York University, working under the guidance of Prof. Justin Cappos. Yuchen earned his Ph.D. from the Department of Computer Science at Stevens Institute of Technology, co-advised by Prof. Jun Xu and Prof. Georgios Portokalidis. Prior to Stevens, Yuchen received his Bachelor's degree in Computer Science at Boston University. His research interests encompass fuzzing, static analysis, system security, and software security, with a current emphasis on Rust programming and software supply chain security. Yuchen’s publications appear in top-tier venues such as USENIX, NDSS, ASE, and FSE. He serves as a co-PI of the NSF POSE Phase II grant (USD 1.5M) and is a Steering Committee member of the OpenSSF sandbox project SBOMit. Yuchen is passionate about crafting innovative approaches to address the evolving challenges in software and system security.