NJIT

Department of Computer Science

Evaluation of Security Controls Toward the Enhancement of Software Supply Chain Security

Nusrat Zahan
North Carolina State University

Hosted by Kasthuri Jayarajah

Date: Monday, March 3, 2025
Coffee: 2:15 PM – 2:30 PM
Time: 2:30 PM – 3:30 PM
Location: GITC 4402 (4th floor Seminar Lecture Hall)
WebEx Link: https://njit-edu.zoom.us/j/91363947764?pwd=bjbvksq2Ylj5hqErxWf1v4F27DhkiY.1

Meeting ID: 913 6394 7764
Passcode: 981752

Abstract:
High-profile supply chain attacks made headlines and directed attention toward the importance of software supply chain security. The attack trends have moved from passive adversaries finding and exploiting vulnerabilities contributed accidentally by well-intentioned developers to a new generation of software supply chain attacks, where attackers inject vulnerabilities directly into dependencies. The US government's concern for the increased security risk posed by supply chain attacks is embodied in Section 4 of Executive Order 14028 and associated guidance on mitigating controls documented in the NIST Secure Software Development Framework (800-218). Industry has also documented security controls, often endorsed by industry groups brought together through the Linux Foundation's Open Source Security Foundation (OpenSSF). As organizations seek to address the escalating risks of software supply chain attacks and comply with government regulations, they can often be overwhelmed by the number of security controls recommended in different security frameworks. To make informed decisions on security control adoption, organizations seek guidance rooted in empirical evidence demonstrating the impact of adopting security controls on project security outcomes.

The research aims to aid software organizations in reducing software supply chain security risk by prioritizing security control adoption through the empirical evaluation of security controls and security outcomes metrics. In this research, we investigate software dependencies as attack vectors. We first study different security metrics to identify potential weak links within the software supply chain and develop an LLM-based code review workflow to detect malicious dependencies. Then, we focus on identifying and evaluating the adoption of security controls that contribute to a strong security posture in software systems. We also investigated security metrics that can be leveraged as security outcome metrics and their relationship with security controls. The underlying assumption is that organizations that prioritize and implement security controls achieve better security outcomes and are better equipped to prevent software supply chain attacks.

Bio:
Nusrat Zahan is a Ph.D. candidate in the Computer Science department at North Carolina State University. Her career goal is to empower software professionals to deliver reliable, resilient, and secure software by bridging the science of software engineering and security with other cross-disciplinary insights from computer science. Her research focuses on measuring security risks, developing actionable security metrics, and leveraging advanced data-driven techniques, including machine learning and large language models, to improve software security. She integrates expertise across diverse domains, including software supply chain security, open-source ecosystems, and artificial intelligence.

Nusrat's research contributions have been adopted by the industry and featured in international press venues. Her work has been published in leading venues such as the International Conference on Software Engineering (ICSE), Mining Software Repositories (MSR) Conference, Empirical Software Engineering (EMSE) Journal, IEEE Security and Privacy Magazine, and the ACM Transactions on Software Engineering and Methodology (TOSEM). She was a research intern at Microsoft Research and Socket. Prior to her doctoral studies, she was a security specialist at NEC Corporation. Nusrat earned her bachelor's degree in Electronics and Communication Engineering from Khulna University of Engineering and Technology.