Seminar

ECU COMPUTER SCIENCE

Enhancing Vulnerability Information Using Automated Analysis

Abstract. Software is complex, not only due to the code within a given project, but also due to the vast ecosystem of open source dependencies and transitive dependencies upon which each project relies. When one of a project's dependencies contains a security vulnerability, the project maintainer must either update the dependency, patch the dependency, or determine that the vulnerability does not affect the project. Unfortunately, vulnerability information is messy and incomplete, making the process of resolving vulnerable dependencies highly manual and error prone. When this manual process is combined with a large number of project dependencies and high rate of vulnerability discovery, project maintainers are left in an untenable position.

Our work seeks to clean up and enrich information in vulnerability databases with the goal of enabling future automated tools that help project maintainers efficiently triage vulnerability reports. First, I will present our efforts to identify security fixes that are not listed in vulnerability databases using a novel approach called Differential Alert Analysis (DAA). Developers often discover and fix vulnerabilities without going through the process of contacting a CVE Numbering Authority (CNA). We applied DAA to a large corpus of per-commit Static Analysis Security Testing (SAST) tool alerts provided by the LGTM project to study silent fixes in NPM, Go, PyPI, and Maven, adding to the public knowledge of vulnerability fixes. Second, I will present our efforts to enhance existing vulnerability advisories with links to commit patches that fix them, also known as vulnerability fixing commits (VFCs). Our VFCFinder tool surpasses prior VFC discovery tools using state-of-the-art Transformers. We incorporate VFCFinder into a larger pipeline to investigate the commits that occur prior to GitHub security advisories to identify previously undocumented patch links. Finally, I will conclude with a discussion of how the information provided by DAA and VFCFinder will support future automated methods of aiding software maintainers in managing vulnerabilities in their project's dependencies

Biography. William Enck is a Professor in the Department of Computer Science at the North Carolina State University where he is co-director of the Secure Computing Institute (SCI) and director of the Wolfpack Security and Privacy Research (WSPR) laboratory. Prof. Enck's research interests span the broad area of systems security with applications to mobile platforms, Internet of Things (IoT), networks, cloud and 5G infrastructure, and the software supply chain. In particular, his work in mobile application security has led to significant consumer awareness and changes to platforms, as well as a SIGOPS Hall of Fame Award. He is currently serving as Secretary for the USENIX Board of Directors, as department editor for IEEE Security and Privacy Magazine, as associate editor for ACM TOPS, and on the steering committee of the USENIX Security Symposium. He was program co-chair of USENIX Security 2018 and is program co-chair of the 2024 and 2025 IEEE Symposium on Security and Privacy (S&P).

Dr. William Enck
Professor
Co-director of the Secure
Computing Institute (SCI)
Dept. of Computer Science
North Carolina State University

whenck@ncsu.edu
https://enck.org

Friday Mar 17, 2023
Time: 2:00 – 3:00pm
Microsoft Teams
Click here to join the meeting

Contact: Dr. Kamran Sartipi
Dept. of Computer Science, ECU
www.cs.ecu.edu/sartipi/CSseminar/